1

ODSJEK PROMET

ZAVOD ZA INFORMACIJSKO-KOMUNIKACIJSKI PROMET

Laboratorij za sigurnost i forenzičku analizu informacijsko-komunikacijskog sustava

Voditelj
Siniša Husnjak, mag. ing. traff.
e-mail: sinisa.husnjak@fpz.hr

DIVISION OF TRANSPORT

DEPARTMENT OF INFORMATION AND COMMUNICATION TRAFFIC

Laboratory for Security and Forensic Analysis of Information and Communication System

Head
Siniša Husnjak, Mag. Ing. Traff.
e-mail: sinisa.husnjak@fpz.hr

1 ODSJEK PROMET
DIVISION OF TRANSPORT

Naziv opreme / Equipment name

Uređaj za forenzičku analizu mobilnih terminalnih uređaja UFED Touch Ultimate Standard
Device for forensic analysis of mobile terminal devices UFED Touch Ultimate Standard

Proizvođač / Manufacturer

Cellebrite Ltd., Petah Tikva, Israel

Namjena i opis / Purpose and description

Tehnološki najnapredniji sustav ekstrakcije, dekodiranja, analize i izvještavanja o podacima na mobilnim uređajima. Uređajem je moguće raditi fizičku, logičku i datotečnu ekstrakciju svih podataka (čak i izbrisanih) iz širokog raspona mobilnih uređaja, uključujući *legacy i featurephone*, *smartphone,* prijenosnih GPS uređaja, tableta te uređaja proizvedenih s kineskim komponentama. S vlastito razvijenim hardverom, integriranom baterijom, intuitivnim grafičkim sučeljem i zaslonom osjetljivim na dodir, UFED Touch Ultimate ubrzava istražni postupak, ispunjavajući stroge zahtjeve forenzičke analize mobilnih uređaja.
UFED Touch Ultimate uređaj dolazi s aplikacijskim paketima:

- UFED Physical Analyzer – napredna aplikacija za dekodiranje, analizu i izvještavanje
- UFED Phone Detective – trenutna identifikacijamobilnog terminalnog uređaja
- UFED Reader – omogućuje autoriziranom osoblju dijeljenje informacija s drugima.

Cutting edge extraction, decoding, analysis and reporting of data on mobile devices. It performs physical, logical, file system and password extraction of all data (even if deleted) from the widest range of devices including legacy and feature phones, smartphones, portable GPS devices, tablets and phones manufactured with Chinese chipsets. With proprietary hardware, an integrated battery, an intuitive GUI and touch screen, the UFED Touch Ultimate speeds up the investigation process, meeting the demands of the mobile forensic industry. The UFED Touch Ultimate solution comes with a range of applications packages:

- UFED Physical Analyzer – The advanced application for decoding, analysis and reporting
- UFED Phone Detective – For instant mobile phone identification
- UFED Reader – Enables authorized personnel to share information with others

Naziv opreme / Equipment name

Prijenosna radna stanica za istraživanje, analizu i testiranje sigurnosti informacijsko-komunikacijskog sustava, Acer Aspire One
Mobile workstation for research, analysis and testing of information and communication system security, Acer Aspire One

Proizvođač / Manufacturer

Acer Inc., New Taipei City, Taiwan

Namjena i opis / Purpose and description

Uređaj se koristi za testiranje sigurnosti, zaštitu, prevenciju napada te analizu prometa informacijsko komunikacijskog sustava. Na uređaju je instalirano Linux Kali sa skupom specijaliziranih alata primjenjivih u svrhu istraživanja, analize i testiranja sigurnosti informacijsko komunikacijskog sustava.
Klase specijaliziranih programskih alata u Linux Kali okruženju:

- prikupljanje informacija
- analiza ranjivosti sustava
- analiza sigurnosti Web aplikacija
- analiza i testiranje sigurnosti bežičnih komunikacijskih mreža
- prisluškivanje, prikupljanje i analiza informacijsko komunikacijskog prometa
- alati za generiranje izvještaja

This device is used for security testing, protection, prevention and analysis of information and communication systems. It uses the Linux Kali environment with a set of specialized tools designed for research, analysis and testing of information and communication systems security.
Classes of specialized software tools in a Linux environment:

- gathering information
- analysis of vulnerability
- web applications security analysis
- analysis and security testing of wireless communication networks

- eavesdropping, collecting and analysis of information and communication traffic
- tools for generating reports

Naziv opreme / Equipment name

Prijenosna radna stanica za administraciju hardverske opreme za mrežnu sigurnost, HP Elitebook 2730p
Mobile workstation for administration of hardware equipment for network security, HP Elitebook

Proizvođač / Manufacturer

Hewlett-Packard Company, Palo Alto, California, USA

Namjena i opis / Purpose and description

Uređaj se koristi za administraciju, konfiguraciju i upravljanje hardverske opreme namijenjene mrežnoj sigurnosti.
Na uređaju se nalaze specijalizirani programski alati:

- za konfiguraciju i upravljanje FortiGate 60D uređajem
- za ostvarenje SSH1 i SSH2 pristupa hardverskim mrežnim uređajima (SuperPutty, OpenSSH)

This device is used for administration, configuration and management of hardware equipment for network security.
The device is equipped with specialized software tools:

- for configuration and management of FortiGate 60D device
- for SSH1 and SSH2 access to hardware network devices (SuperPutty, OpenSSH)

Naziv opreme / Equipment name

Prijenosna radna stanica za administraciju hardverske opreme za mrežnu sigurnost, HP Pavilion dm1
Mobile workstation for research, analysis and testing of information and communication system security, HP Pavilion dm1

Proizvođač / Manufacturer

Hewlett-Packard Company, Palo Alto, California, USA

Namjena i opis / Purpose and description

Uređaj se koristi za testiranje sigurnosti, zaštitu, prevenciju napada i analizu sigurnosti informacijsko-komunikacijskog sustava. Na uređaju je instalirano Linux Backbox okruženje sa skupom specijaliziranih alata primjenjivih u svrhu penetracijskih testiranja i procjene sigurnosti informacijsko-komunikacijskog sustava što uključuje i VoIP infrastrukturu, bežičnu I lokalnu komunikacijsku infrastrukturu.
Klase specijaliziranih programskih alata u Linux Backbox okruženju:

- dokumentiranje i izvještaji
- reverzni inženjering
- socijalni inženjering
- forenzička analiza
- VoIP analiza
- analiza bežičnih komunikacijskih mreža

This device is used for security testing, protection, prevention and analysis of information and communication systems. It uses the Linux Backbox environment with a set of specialized tools for penetration testing and security assessment of information and communication systems, including VoIP infrastructure and wireless and local communications infrastructure.
Classes of specialized software tools in the Linux Backbox environment:

- documentation & Reporting
- reverse Engineering

- social Engineering
- forensic Analysis
- VoIP Analysis
- wireless Analysis

Naziv opreme / Equipment name

Uređaj za sigurnost, zaštitu i forenzičku analizu mrežnog informacijsko-komunikacijskog prometa, AirPort Time Capsule
Device for security, protection and forensic analysis of network communication traffic, AirPort Time Capsule

Proizvođač / Manufacturer

Apple, California, USA

Namjena i opis / Purpose and description

Uređaj se koristi za sigurnosna testiranja, zaštitu, prevenciju i forenzičku analizu informacijsko-komunikacijskog prometa.
Karakteristike uređaja:

- IEEE 802.11a/b/g/n/ac povezivost
- snopovsko antensko područje
- simultano korištenje 2.4 GHz i 5 GHz frekvencijskog područja
- 3x brži, jači i kvalitetniji Wi-Fi signal
- simultano višekorisničko iskustvo
- povećan broj antenskih sustava
- ugrađen upravljački asistent
- siguran pristup eksternom USB tvrdom disku
- vatrozid
- zaštita mreže od zlonamjernih napada

This device is used for security testing, protection, prevention and forensic analysis of information and communication traffic.
Device characteristics:

- IEEE 802.11a/b/g/n/ac
- beamforming antenna array

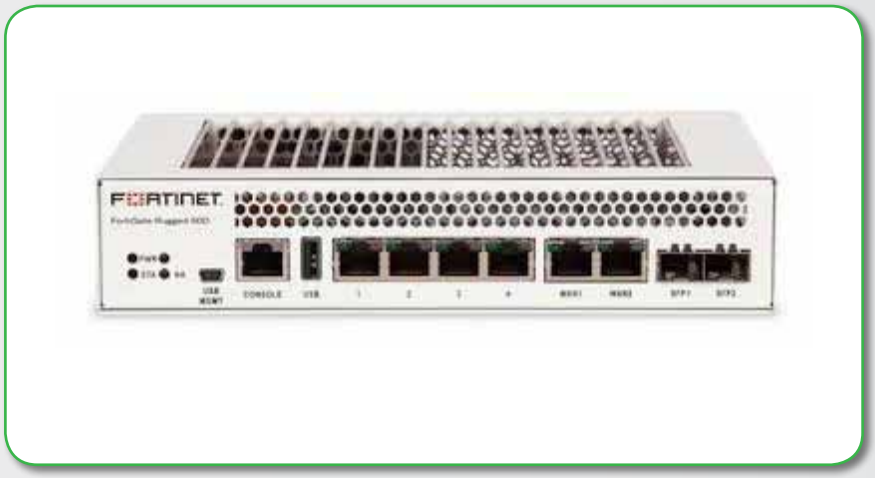
- simultaneous dual-band 2.4 GHz and 5 GHz
- 3x faster Wi-Fi and a stronger, clearer signal
- simultaneous multi-user
- increased number of antennas
- built-in setup assistant
- secure external USB hard drive
- built-in firewall
- network protection from malicious attacks

Naziv opreme / Equipment name

Uređaj za sigurnost, zaštitu i forenzičku analizu mrežnog informacijsko-komunikacijskog prometa, FortiGate 60D
Device for security, protection and forensic analysis of network communication traffic, FortiGate 60D Hardware

Proizvođač / Manufacturer

Fortinet Inc., California, USA



Namjena i opis / Purpose and description

Uređaj se koristi za sigurnosna testiranja, zaštitu, prevenciju i forenzičku analizu informacijsko-komunikacijskog prometa.
Karakteristike uređaja:

- napredne mogućnosti zaštite
- vatrozid
- kontrola aplikativnih paketa
- prevencija neovlaštenih napada
- virtualne privatne mreže
- filtriranje web sadržaja
- sigurnost mobilnih terminalnih uređaja
- identifikacija uređaja
- upravljanje pristupom i sigurnosnim politikama (BYOD)
- segmentacija mreže

This device is used for security testing, protection, prevention and forensic analysis of information and communication traffic.
Device characteristics:

- advanced threat protection
- firewall

- application control
- IPS (Intrusion Prevention System)
- VPN (Virtual Private Networks)
- web filtering
- mobile devices security
- devices identification
- customizable access and security policies (BYOD)
- networks segmentation

1 ODSJEK PROMET
DIVISION OF TRANSPORT

Naziv opreme / Equipment name

Uređaj za sigurnost, zaštitu i forenzičku analizu mrežnog informacijsko-komunikacijskog prometa, FortiAP 221C Indoor wireless AP
Device for security, protection and forensic analysis of network communication traffic, FortiAP 221C Indoor wireless AP

Proizvođač / Manufacturer

Fortinet Inc., California, USA

Namjena i opis / Purpose and description

Uređaj se koristi za sigurnosna testiranja, zaštitu, prevenciju i forenzičku analizu informacijsko-komunikacijskog prometa.
Karakteristike uređaja:

- siguran pristup WiFi mreži temeljen na identitetima
- zaštita mreže od strane naprednih napada
- dubinska (L7) analiza za preciznu kontrolu aplikacija i korištenja frekvencijskog pojasa
- središnje upravljanje
- softverska integracija radi središnjeg upravljanja i izvještavanja
- dvostruki radio link 802.11ac pristupnoj točci
- identifikacija gostujućih WiFi pristupa
- detektor dima
- dvostruki radio link i prijenosna širina
- simultane klijentske konekcije

This device is used for security testing, protection, prevention and forensic analysis of information and communication traffic.
Device characteristics:

- secure, identity-driven WiFi access
- network protection from advanced wireless threats

- deep Layer 7 inspection to precisely control applications and bandwidth usage
- central management
- software integration for centralized management and reporting
- dual-radio 802.11ac AP
- guest or social WiFi deployments
- smoke detector
- dual-radio and dual-band
- simultaneous client connections

Naziv opreme / Equipment name

Uređaj za sigurnost, zaštitu i forenzičku analizu informacijsko-komunikacijskog prometa, Samsung Galaxy S6 Edge+
Device for security, protection and forensic analysis of information and communication traffic, Samsung Galaxy S6 Edge+

Proizvođač / Manufacturer

Samsung Inc., Seoul, South Korea

Namjena i opis / Purpose and description

Uređaj se koristi za sigurnosna testiranja, zaštitu, prevenciju i forenzičku analizu informacijsko-komunikacijskog prometa.
Karakteristike uređaja:

- GSM / HSPA / LTE mobilne komunikacijske tehnologije
- HSPA 42.2/5.76 Mbps, LTE Cat6 300/50 Mbps/ LTE Cat9 450/50 Mbps
- Android OS, v5.1.1 (Lollipop)
- Četvero-jezgreni 1.5 GHz Cortex-A53 i četvero-jezgreni 2.1 GHz Cortex-A57
- Wi-Fi 802.11 a/b/g/n/ac, dual-band, Wi-Fi Direct, hotspot
- A-GPS, GLONASS, BDS
- sigurnosne i senzorske značajke: otisak prsta, akcelerometar, žiroskop, prisutnost, kompas, barometar, otkucaji srca, SpO2
- upravljanje i mjerenje ostvarenja mobilnog i mrežnog podatkovnog prometa
- sigurnosne značajke mobilnog i mrežnog podatkovnog prometa

This device is used for security testing, protection, prevention and forensic analysis of information and communication traffic.
Device characteristics:

- GSM / HSPA / LTE mobile communication technologies
- HSPA 42.2/5.76 Mbps, LTE Cat6 300/50 Mbps/ LTE Cat9 450/50 Mbps

- Android OS, v5.1.1 (Lollipop)
- Quad-core 1.5 GHz Cortex-A53 & Quad-core 2.1 GHz Cortex-A57
- Wi-Fi 802.11 a/b/g/n/ac, dual-band, Wi-Fi Direct, hotspot
- A-GPS, GLONASS, BDS
- security and sensors: fingerprint, accelerometer, gyro, proximity, compass, barometer, heart rate, SpO2
- measurement and management of mobile and network data traffic usage
- security of mobile and network data traffic

Naziv opreme / Equipment name

Radna stanica za forenzičku analizu mobilnih terminalnih uređaja te SIM kartica, HP Pro 3420 AiO
Workstation for forensic analysis of mobile terminal devices and SIM cards, HP Pro 3420 AiO

Proizvođač / Manufacturer

Hewlett-Packard Company, Palo Alto, California, USA

Namjena i opis / Purpose and description

Uređaj se koristi za forenzičku analizu informacijsko-komunikacijskog prometa i pohranjenih podataka mobilnih terminalnih uređaja te SIM kartica.
Karakteristike uređaja:

- fizička i logička ekstrakcija podataka
- ektrakcija datotečnog sustava
- ekstracija zaporki, postojećih, obrisanih ili skrivenih podataka
- ekstrakcija i kloniranje SIM kartica
- upravljanje izvještajima
- broj radnih stanica: 2

Popis instaliranih specijaliziranih programskih alata za forenzičku analizu mobilnih terminalnih uređaja:

- UFED Viewer
- MobilEdit! Forensic
- Phone Forensic Express

Device is used for forensic analysis of information and communication traffic and saved data on mobile terminal devices and SIM cards.
Device characteristics:

- physical and logical data extraction

- file system data extraction
- passwords, viewable, deleted or hidden data extraction
- SIM card data extraction and SIM cloning
- report management
- number of workstations: 2

List of installed specialised software tools for forensic analysis of mobile terminal devices:

- UFED Viewer
- MobilEdit! Forensic
- Phone Forensic Express

Naziv opreme / Equipment name

Radna stanica za forenzičku analizu mobilnih terminalnih uređaja, Lenovo 6068CPO
Workstation for forensic analysis of mobile terminal devices, Lenovo 6068CPO

Proizvođač / Manufacturer

Lenovo Group Limited, Beijing, China

Namjena i opis / Purpose and description

Uređaj se koristi za forenzičku analizu informacijsko-komunikacijskog prometa i pohranjenih podataka mobilnih terminalnih uređaja.
Karakteristike uređaja:

- logička ekstrakcija podataka
- ektrakcija datotečnog sustava
- ekstracija zaporki, postojećih ili skrivenih podataka
- upravljanje izvještajima
- broj radnih stanica: 2

Popis instaliranih specijaliziranih programskih alata za forenzičku analizu mobilnih terminalnih uređaja:

- Phone Forensic Express
- Paraben Device Seizure
- Mobilyze

Device is used for forensic analysis of information and communication traffic and saved data on mobile terminal devices.
Device characteristics:

- logical data extraction
- file system data extraction

- passwords, viewable or hidden data extraction
- report management
- number of workstations: 2

List of installed specialised software tools for forensic analysis of mobile terminal devices:

- Phone Forensic Express
- Paraben Device Seizure
- Mobilyze