

SADRŽAJ:

1. UVOD	5
2. GNU/LINUX OPERATIVNI SISTEM	6
2.1 Istorija <i>Linux</i> -a	7
2.2 Koncept GNU/Linux operativnog sistema	8
2.2.1 Nivoi i slojevi apstrakcije u Linux sistemu	9
2.2.2 Hardver – razumijevanje glavne memorije	11
2.2.3 Kernel (jezgro)	11
2.3 Distribucije Linux sistema.....	14
2.4 Prednosti i nedostaci GNU/Linux operativnih sistema	16
3. ANDROID OPERATIVNI SISTEM	20
3.1 Arhitektura Android operativnog sistema	21
3.2 Upravljanje procesima.....	23
3.3 Raspoređivanje procesorskih (CPU) resursa	27
3.4 Upravljanje radnom (RAM) memorijom.....	28
3.5 Upravljanje skladišnim prostorom (HDD/SSD).....	31
3.6 I/O upravljanje.....	32
3.7 Optimizacija baterije	34
3.8 Verzije Android operativnog sistema.....	36
4. ANDROID FORENZIKA	44
4.1 Proaktivna forenzička istraga	45
4.2 Reaktivna forenzička istraga	48
4.3 Izazovi u Android forenzici	49
4.3.1 Izazovi zasnovani na aplikacijama	50
4.3.2 Izazovi zasnovani na dozvolama	51
4.3.3 Izazovi zasnovani na ekstrakciji podataka.....	52
4.4 Alati za forenziku Android mobilnih platformi	54
4.4.1 Andriller	55
4.4.2 XRY	56
4.4.3 UFED.....	57
4.4.4 <i>OXYGEN Forensics</i>	58
4.4.5 <i>MOBILedit Forensics</i>	59
4.4.6 <i>DroidSpotter</i>	60
4.4.7 <i>Volatility</i>	61
4.4.8 <i>MPE+</i>	62
4.4.9 <i>viaExtract</i>	63
4.4.10 <i>MSAB</i>	64
4.5 Sistemi za forenziku Android mobilnih platformi.....	64
4.5.1 <i>Santoku 0.5</i>	65
4.5.2 <i>Tsurugi 2023.2</i>	68
4.5.3 <i>Ubuntu 22.04 LTS</i> i „ <i>ALEAPP</i> “	70
5. ZAKLJUČAK	72
6. LITERATURA	73
7. SPISAK SKRAĆENICA	75

Raspored slika:

Slika 1 - Organizacija Linux sistema.....	10
Slika 2- Pokretanje novog procesa	13
Slika 3 - Kernel (jezgro) i Startup proces za Android	23
Slika 4 - Pokrenuti procesi.....	24
Slika 5 - Manualno upravljanje procesima	25
Slika 6 - Automatsko upravljanje procesima	26
Slika 7 - Primjer Deadlock-a.....	27
Slika 8 - Upravljanje RAM memorijom	29
Slika 9 - Aplikacije u stanju Standby	30
Slika 10 - Pregled upotrebe memorije od strane aplikacija	31
Slika 11 - Direktorijumski raspored i struktura u Android operativnom sistemu	32
Slika 12 - Podešavanja privatnosti	34
Slika 13 - Podešavanja baterije	35
Slika 14 - Android logo	43
Slika 15 - Neuspjeh aplikacije Andriller.....	51
Slika 16 - Permisijski neuspjeh aplikacije Andriller	52
Slika 17 - Analiza slike memorije pomoću alata Sleuthkit.....	53
Slika 18 - Email adrese prikupljene pomoću Sleuthkit-a	54
Slika 19 - Slike prikupljene alatom Sleuthkit-a iz metapodataka	54
Slika 20 - Andriller UI.....	56
Slika 21 - XRY UI.....	57
Slika 22 - UFED Physical Pro.....	58
Slika 23 - Oxygen Forensics Detective	59
Slika 24 - Mobile Forensics PRO UI.....	60
Slika 25 - DroidSpotter UI.....	61
Slika 26 - Volatility u Ubuntu Power Shell-u	62
Slika 27 - MPE+	62
Slika 28 - viaExtract UI.....	63
Slika 29 - XAMN UI	64
Slika 30 - Santoku 0.5 UI	67
Slika 31 - Android Triage set alata	69
Slika 32 - Tsurugi 2023.2 UI.....	70
Slika 33 - ALEAPP UI.....	71

Raspored tabela:

Tabela 1 - Razlike između Linux-a i Unix-a.....	18
Tabela 2 - Razlika između Linux-a i Windows-a.....	19
Tabela 3 - Arhitektura Android operativnog sistema.....	22
Tabela 4 - Verzije Android sistema u upotrebi.....	43