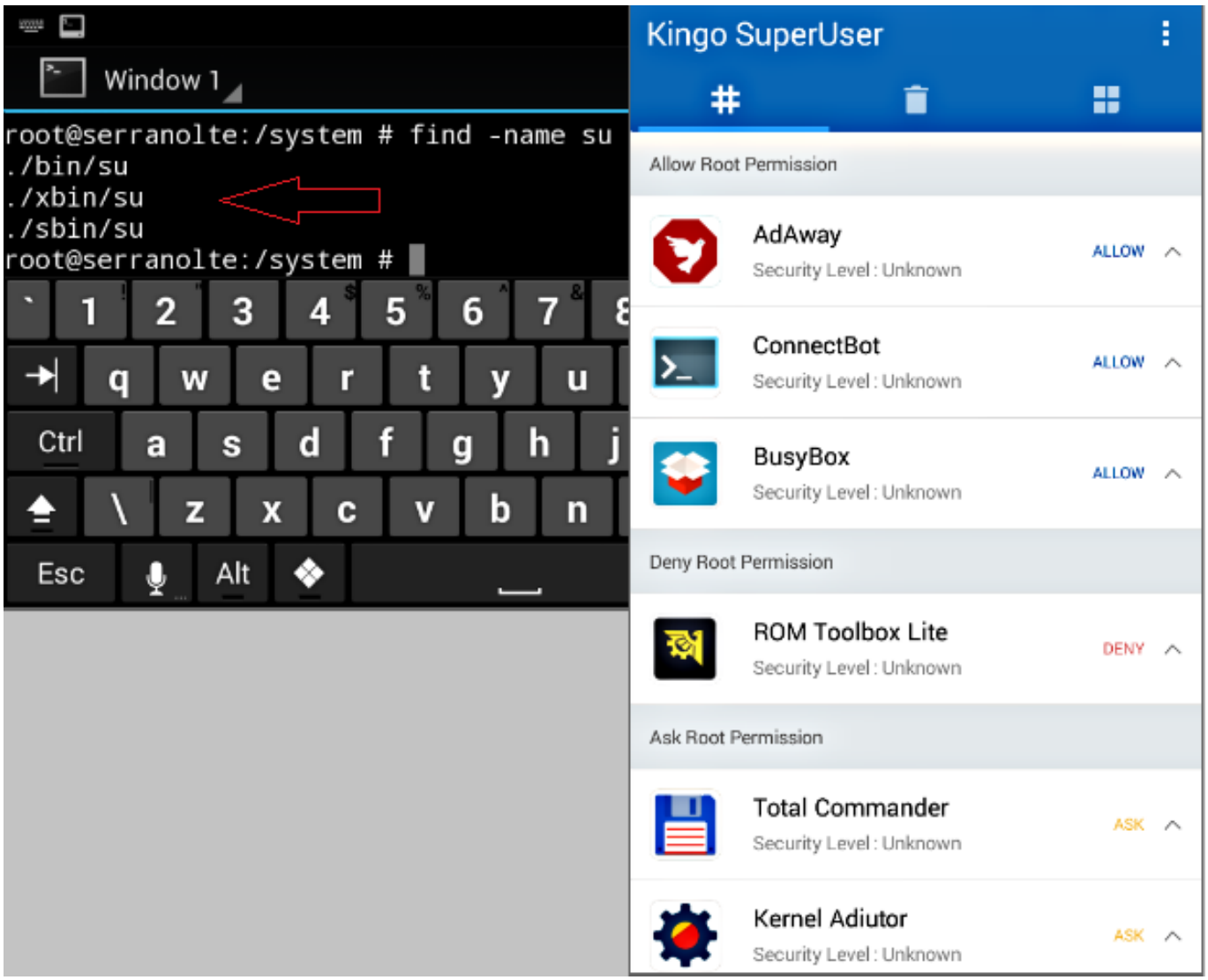
Android uređaji - rootati ili ne, pitanje je sad

Prethodni članci o optimizaciji Android uređaja pokazali su da se mnogo prilagodbi može odraditi s ovlastima običnog korisnika. Treba se upoznati s bitnim značajkama Android platforme - tipično, upravljanje radnom memorijom i aplikacijama, uloga određenih particija, međuzavisnosti ključnih komponenti – i tada možemo, služeći se raspoloživim alatima OS-a, pratiti ponašanje hadverskih i softverskih modula te na uređaj djelovati ne samo na esteskoj, nego i na funkcionalnoj, performansnoj i sigurnosnoj razini. Oni zahtjevniji posegnut će za dodatnim alatima, s kojima mogu steći bolji uvid u stanje svake pojedine komponente i prodornije utjecati na njeno ponašanje.

Posebna smo kategorija mi malobrojni koji želimo potpunu kontrolu nad Android uređajem. Što će reći – prava superusera, roota. A takvi su „šaka u oko“ proizvođačima Android uređaja i telekom operaterima. Smatram nekorektnim prpričavati općepoznato, zato kao podsjetnik nudim link [1] na članak iz 2011. godine, zanimljiv radi objektivnosti i lucidnosti autora i spoznaje da se ništa bitno nije promijenilo u tom području.

Ako želimo postati root - po naški: faca :o) - uređaj moramo rootati, a u pravilu to neće ići bez otključavanja bootloadera. Onog sekundarnog, primarni je u ASIC čipu pa je, posljedično, "needitabilan". Otključavanje bootloadera možemo izvesti uz podršku proizvođača poput LG, HTC, Sony (dakako, oni postavljaju svoja pravila igre) ili bez te podrške. Samsung je najrazvikaniji predstavnik nekooperativne struje. Potom slijedi rootanje - to je u stvari ugnježđivanje SU komandnog modula u određene direktorije particije /system - te instalacija neke aplikacije tipa SuperUser posredstvom koje drugim aplikacijama dodjeljujemo ili branimo uporabu SU modula.



Osmišljavanje metoda i izrada alata za rootanje izuzetno je zahtjevan posao; ljudi koji se time bave – sve vrsni developeri - ulažu mnogo truda i vremena jer u osnovi rade na otkrivanju i iskorištavanju slabosti aktualnog mehanizma zaštite bootloadera. Tim ljudima, okupljenima u (ne)formalne grupe, stalo je do popularizacije rootanja jer time se potvrđuje njihov „way of life“, još važnije, stvaraju se prilike za neku zaradu. Zbog toga na njihovim Internet stranicama možemo naći prave ode o dobrobitima rootanja, dopadljive floskule o pozitivnoj korelaciji između slobode i superuser prava.... a nedostaci se samo ovlaš spominju ili čak ignoriraju.

Osobno rootam svoje Android uređaje (svoje, ne službene), ali ne radim to zbog uvažavanja spomenutih hvalospjeva nego zato što smatram da se kao sistemac-profesionalac moram dostatno zbližiti s Android temama & dilemema. No, taj imperativ profesionalnosti nameće mi i objektivno sagledavanje teme. Utoliko, kad sam pitan o svrhovitosti rootanja, koristim ovaj pristup:

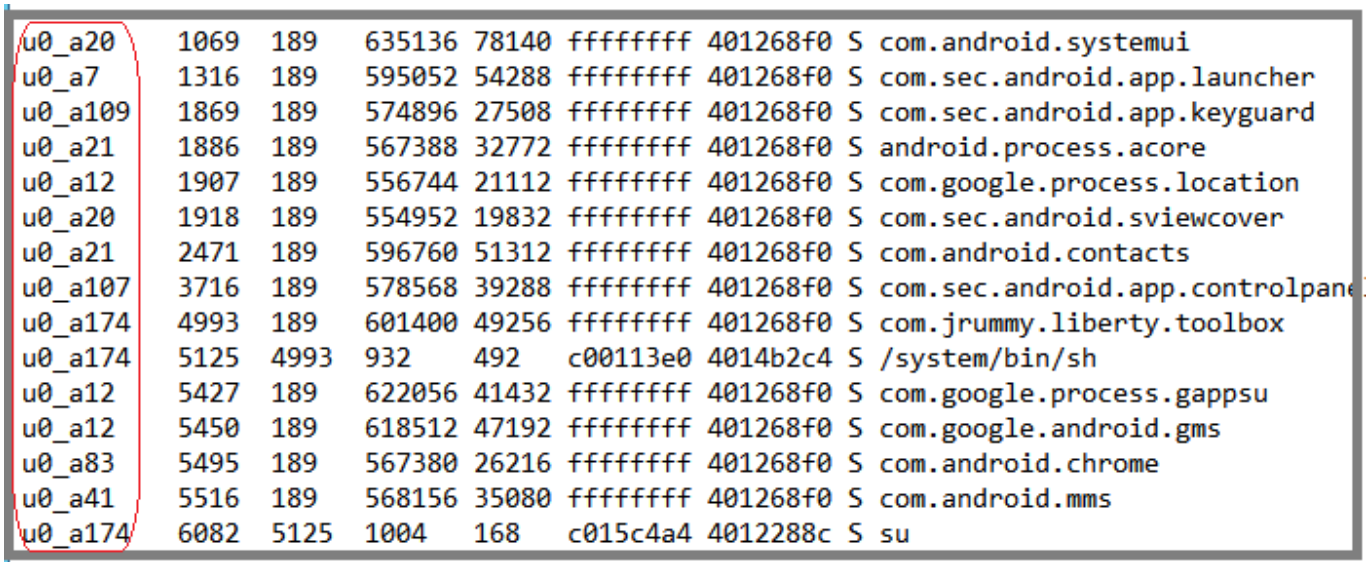
a) preporučim sugovorniku da pročita članak na ovom linku [2] uz napomenu: „Rootanjem posao ne završava nego počinje, dakle, ako nemaš volje ovo izrecitirati napamet u bilo kojem trenutku, status superusera nije ti potreban.“;

b) proces rootanja može loše završiti, treba se dooobro pripremiti (vidi niže);

c) objasnim da se rootanjem negativno utječe na sandboxing kao ključni sigurnosni model (procesi određene aplikacije mogu pristupati samo svojim podacima i u RAM-u i na „disku“), štoviše, otvara se prostor za kompromitaciju samog kernela.

Glede naredne slike: Iako Android nema passwd/shadow, pun je UID-ova jer svaka aplikacija trenutkom instalacije dobije svoj identitet. Kombinacija UID-ova, izolacije procesa i restriktivnih prava

na razini datotečnog sustava onemogućuje aplikacije u dijeljenju procesa i podataka (osim ako se ne potpišu istim privatnim ključem, jer svaka je aplikacija digitalno potpisana).



Upravo točku c) minoriziraju ili prešućuju zagovornici rootanja. Rootanjem, kao završnim činom invazivnog prodora u AOS, uređaj postaje manje otporan na provale kroz USB i Wi-Fi/Data konekcije. Istina je da SuperUser aplikacijom možemo odbijati upite za eskalacijom privilegija, ali nitko nam ne garantira da je ta aplikacija neranjiva ili nezaobilazna. Nemamo niti neporecivo jamstvo da se alat za rootanje ne može zlorabiti za upad u uređaj. Temeljni postulat sigurnosti je nepovjerenje, stoga, ukoliko konkretan Android uređaj rabimo u poslovne svrhe, za financijske transakcije, čuvamo na njemu sigurnosno osjetljive podatke i slično, uistinu nam je isplativije ne rootati ga.

Dodatan je problem rootanog uređaja neotpornost na aplikacije s programskim bugovima, te na one aplikacije koje preagresivno izvršavaju svoju misiju. Vaš autor je jednom prilikom na rootani Galaxy S4 instalirao aplikaciju sa Google Play jer ga je zainteresiralo zbog čega ima tako visok rejting. Ta moja znatiželja završila je flashanjem službenog ROM-a jer je nakon instalacije aplikacije baterija telefona počela „gorjeti“, a deinstalacija te aplikacije ostavila je uređaj u poluoperativnom stanju.

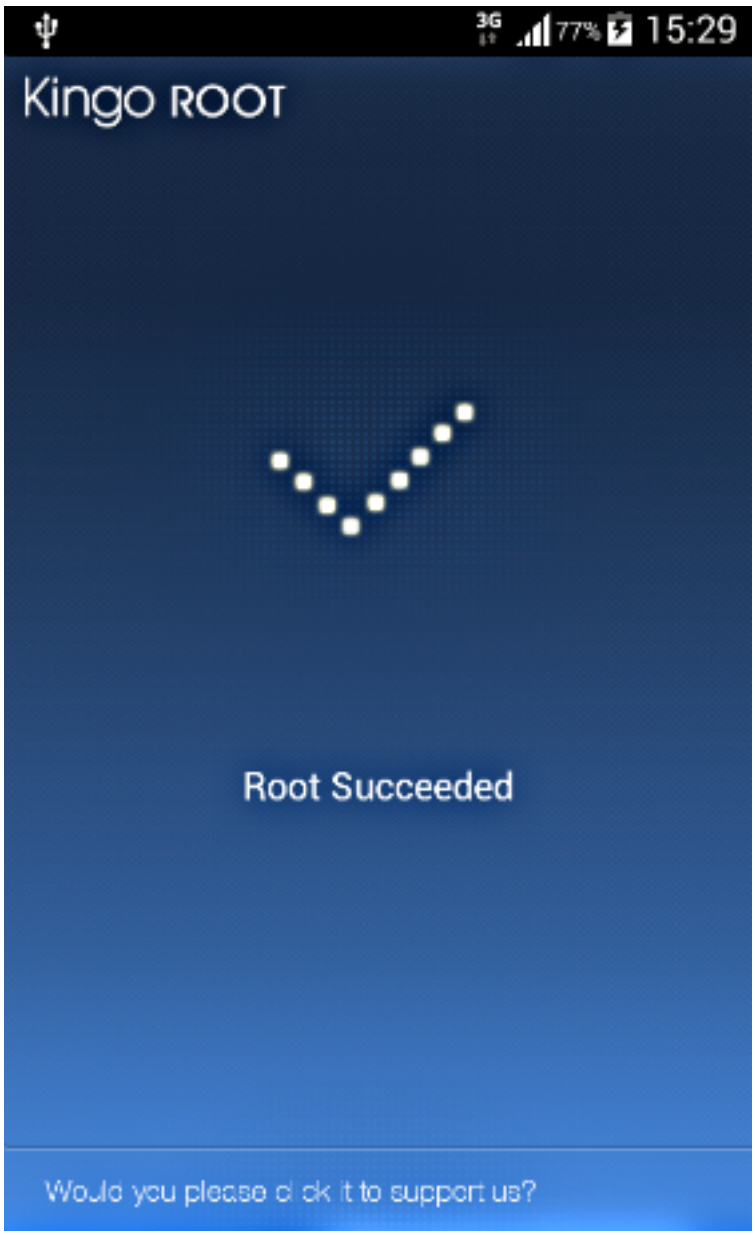
* Sad ćemo razraditi točku b), znači, slijedi par konkretnih savjeta za rootanje Android uređaja:

1. Backupirati (doosadnoo) sve što želimo sačuvati jer postoje modeli smartphonea i tableta kod kojih se tijekom rootanja mora odraditi Factory Reset a njime se brišu sve naše aplikacije i podaci (e, sad više nije dosadno).

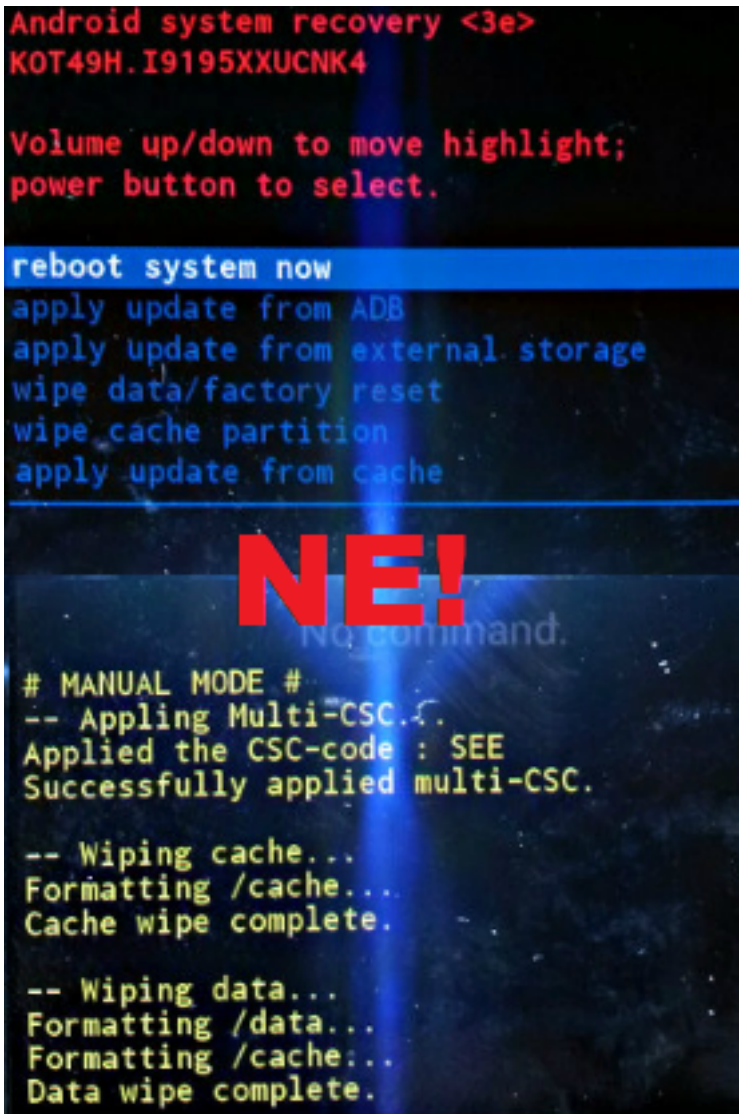
2. Opskrbiti se originalnim firmwareom ili službenim ROM-om, i jasnim uputama za instaliranje (flashanje) tog ROM-a. S ovim „borbenim kompletom“ izvući ćemo se iz svake nevolje koju nam priredi neuspješno rootanje.

3. Na portalu proizvođača uređaja provjeriti što se može odraditi uz njihovu podršku jer, kako znamo, neki od njih omogućuju otključavanje bootloadera. Potom provjeravamo koje bi nam softversko rješenje za rootanje najviše odgovaralo s obzirom na model našeg uređaja i aktualnu verziju AOS-a. Ponuda je, kako to već biva u Android areni, šarena. S jedne su strane specijalizirani tzv. one-click alati poput iRoot, Kingo Root, Towel, Wondershare...., s druge strane su step-by-step alati poput ADB i FastBoot. Jedan od kriterija za konačni odabir neka bude i sposobnost alata da odradi unrootanje uređaja.

4. Koji god alat odabrali, kad ga jednom instaliramo – ili na PC ili direktno na uređaj – i pokrenemo, pažljivo ćemo slijedite njegove upute. Štoviše, kako bismo umanjili mogućnost lošeg ishoda, isključit ćemo A/V softver te alatu osigurati internet konekciju, čak i ako to nije istaknuto.
Po završetku rootanja dobit ćemo, nadajmo se, situaciju poput ove na nižoj slici.



Ali što ako rootanje ne uspije pa uređaj ne ide dalje od bootloadera, ili se digne ali posrće?! Nipošto ne pokrećite Factory reset ili opcije Wipe-ovo-i-ono iz Recovery konzole, znači, nemojte raditi kako je niže prikazano!



Prisjetite se da smo se u etapi priprema opskrbili originalnim ROM-om i uputama kako ga primijeniti. Slijedi procedura vraćanja Samsungovog Galaxy S4 u funkciju nakon neuspješnog rootanja. Ovim postupkom sačuvat ćemo sve naše aplikacije, podatke i prilagodbe sustava. Zgodno, zar ne?! :o)

Instalirati Samsungov USB driver, trenutna verzija je 1.5.x.

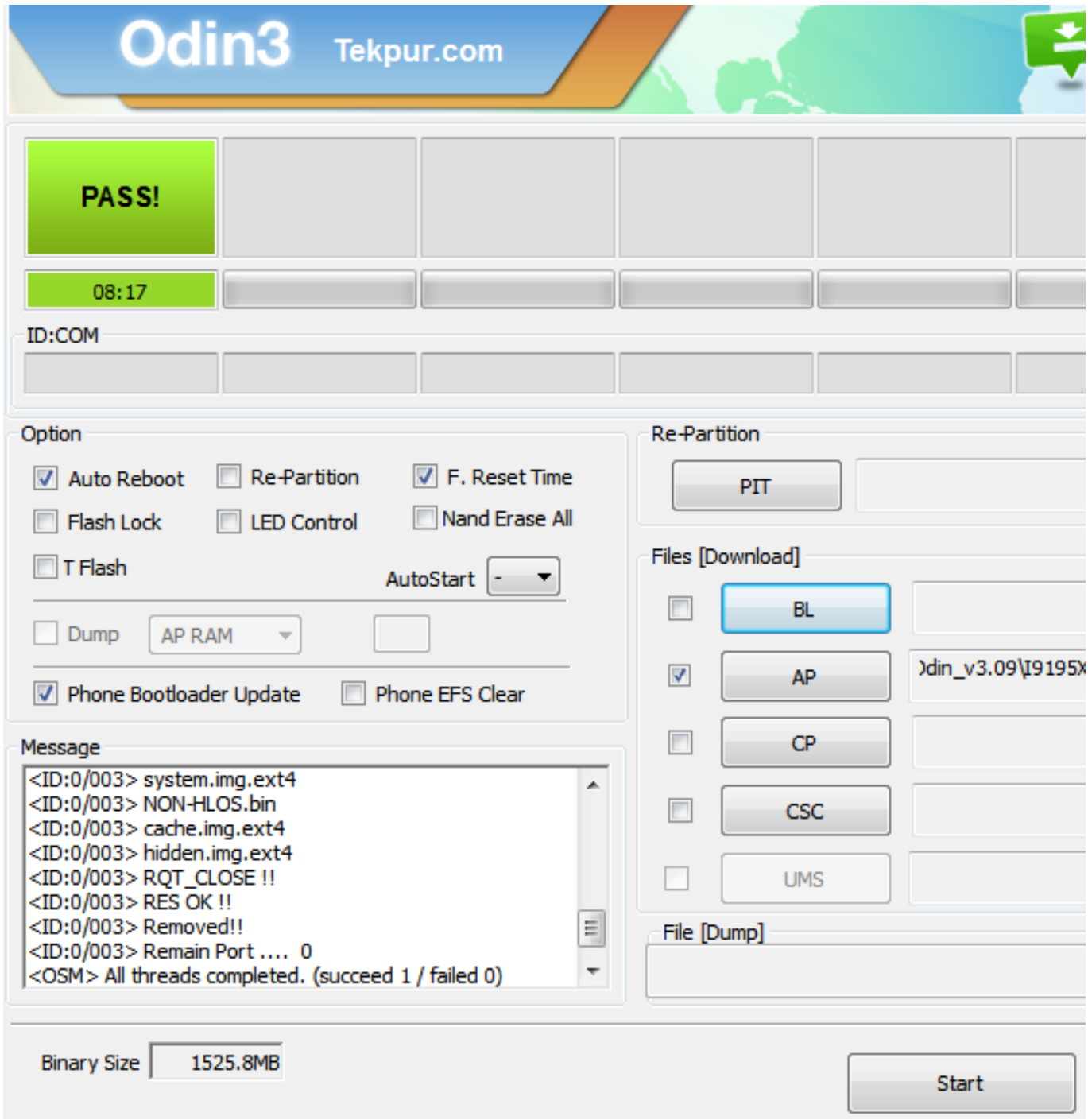
Odin v.3.9, softver za flashanje i rootanje Samsungovih uređaja, samo raspakiramo u neki folder PC-a.
U Odinov direktorij staviti raspakirani ROM tipa .tar (Odin ne radi sa zip formatom), i prateći .dll.

Iz S4 izvaditi bateriju, nakon minutu vratiti.

Postaviti S4 u tzv. Odin mode sekvencom: prvo tipka Volume down, pa Power pa Home (intervali sekvence moraju biti kratki).

Spojiti telefon i PC USB kabelom i pričekati da se učita driver.
Odin pokrenuti sa Run as Administrator, pričekati da prepozna uređaj... dalje kao na slici: u polje AP učitati ROM, uključiti Phone bootloader update.

Dok se telefončić reanimira, razmisliti koji alat i/ili postupak iskoristiti za novi pokušaj rootanja. ;-)



sri, 2016-03-23 14:02 - Ratko Žižek**Kuharice:** Android [3]
Kategorije: Software [4]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Source URL: https://sysportal.carnet.hr/node/1629

Links

[1] http://www.androidcentral.com/bootloaders-all-you-ever-wanted-know
[2] https://community.freescale.com/docs/DOC-102546
[3] https://sysportal.carnet.hr/taxonomy/term/64
[4] https://sysportal.carnet.hr/taxonomy/term/25