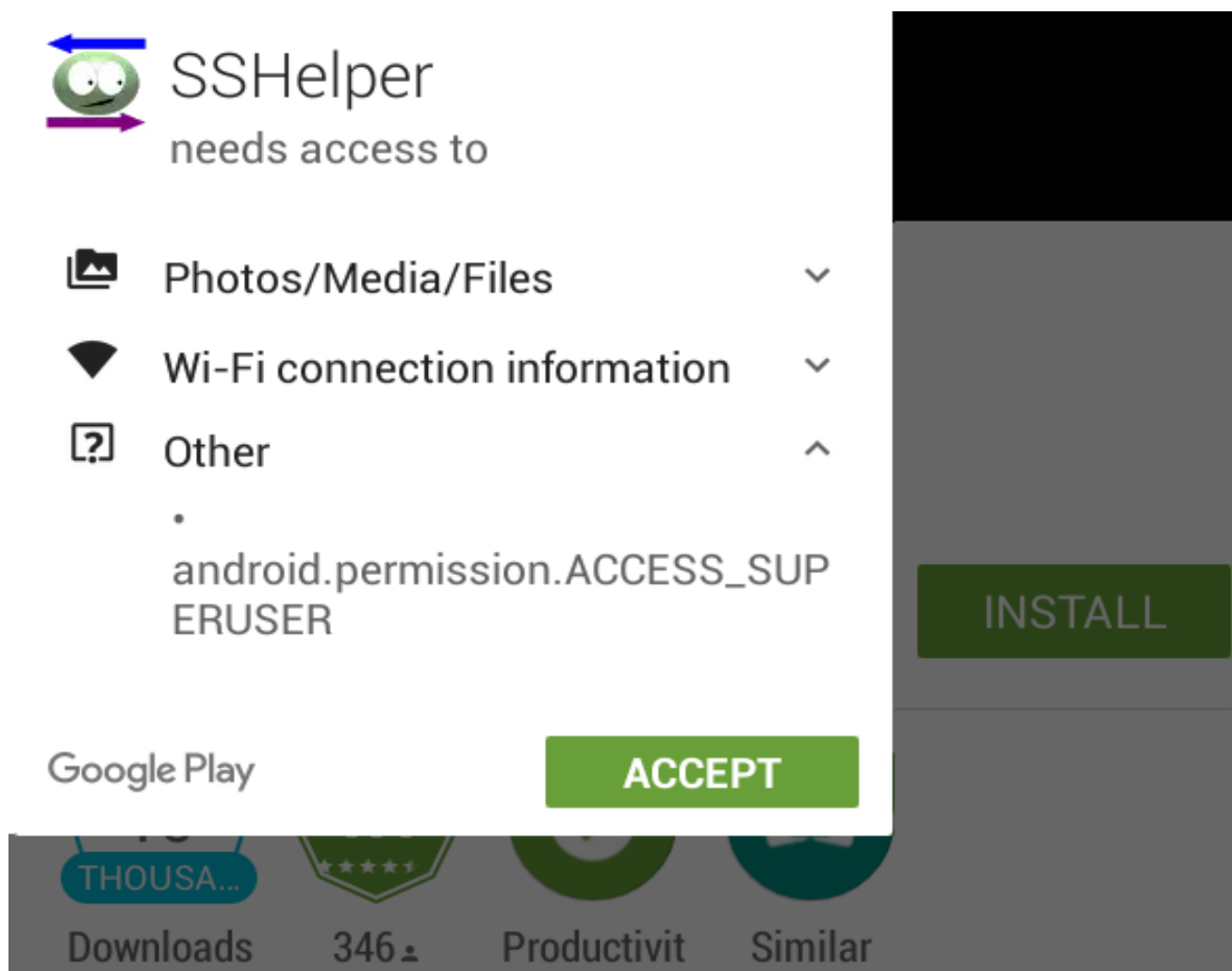


SSHHELPER - Secure shell server za Android



Mobilni uređaji s tvorničkom (stock) edicijom Android OS-a raspolažu s vrlo skromnim fondom komandnolinijskih alata. Jedan od bolno nedostajućih je i SSH u svom serverskom i klijentskom aspektu, znači, bez instalacije dodatnog softvera na Android uređaju ne možemo podići SSH servis ili rabiti naredbe poput ssh, scp, sftp, rsync.... SSH tehnologija dokazani je „numero uno“ za siguran prijenos većih količina podataka između umreženih računala i za administriranje udaljenih računala, pa prije ili kasnije neki SSH produkt ipak sjedne na Android spravice informatičara i naprednih korisnika.

Što se tiče klijentskog dijela SSH suite, Google dućan i slični mu repozitoriji Android aplikacija ponudit će nam solidan izbor alata, ali traganje za dobrim Android SSH serverom na kraju se svede na "izbor" - ili SSHelper ili ništa. Po mišljenju vašeg autora, dakako. Ovako razmišljam: za razliku od braće mu po namjeni, SSHelper se kontinuirano unapređuje i prilagođava novim verzijama AOS-a, dobro je dokumentiran, resursno skroman i pouzdan, ujedno zaista besplatan jer košta nula kuna, a ne prikazuje reklame. U prilog mu ide i jako dobar status njegovog autora u zajednici Android developera. Tijekom instalacije vidjet ćemo da aplikacija traži minimum dozvola na sustav, što je još jedan pozitivan pokazatelj njene kvalitete.



Stavka ACCESS_SUPERUSER prikazana na prethodnoj slici pojavljuje se samo tijekom instalacije na rootani Android uređaj. SSHelper normalno radi na nerootanom AOS-u samo što tada ne možemo SSH servis i web usluge što ih aplikacija nudi (log servisa i clipboard) postaviti na portove niže od 1024, također, bez dosta komplicirane rekonfiguracije SSH servis ne može pristupiti eksternom spremištu podataka. Što se tiče portova, budući da SSH klijenti uglavnom omogućuju kreiranje konektora s predefiniranim parametrima, nestandardni portovi poput defaultnog TCP 2222 na kojem sluša SSH daemon SSHelpa uopće nisu problem. Vaš autor vrti jedan SSHelper na rootanom uređaju ali nije mijenjao niti jedan predefinirani visoki port jer jednostavno nema potrebe za time. SSHelper instalirajte ulogirani na Android kao primarni korisnik, owner. Evo koje funkcionalnosti dobijamo:

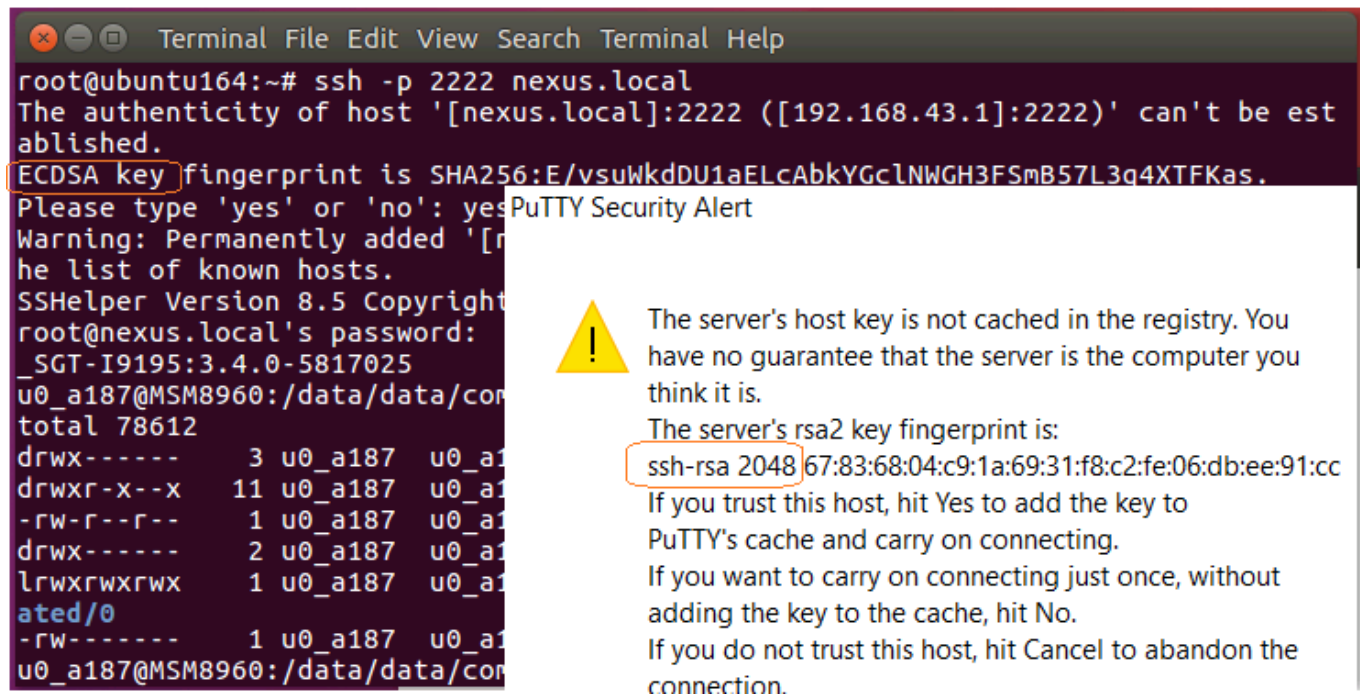
- SSH servis s podrškom za ssh, scp, sftp i rsync protokole, predefinirani port je TCP 2222;
- web usluga za odabir i pregledavanje logova, sluša na portu TCP 8080;
- web usluga za razmjenu tekstualnih podataka između SSH servera i admin stanice posredstvom AOS-ovog clipboarda, sluša na portu TCP 8081;
- Busybox s brojnim naredbama dohvatljivim kroz simbolične linkove (pa ne moramo tijekom pokretanja naredbe eksplicitno pozivati Busybox) i solidan terminal za komandnolinijski rad lokalno ili na drugom SSH serveru;
- pregledan lokalni help sa informacijama o mogućim prilagodbama SSH hosta ili admin računala, sve kako bismo se što brže mogli prihvatiti nekog konkretnog posla.

Naredna slika pokazuje high-level konfiguraciju mog kućnog SSH servera.

SSH server port number:	2222
Log server port number:	8080
Clipboard server port number:	8081
Server Password:
Disable password logins:	<input type="checkbox"/>
Enable strict modes:	<input checked="" type="checkbox"/>
Allow port forwards from any host:	<input type="checkbox"/>
Run SSHelper service at boot:	<input checked="" type="checkbox"/>
Check Network connectivity:	<input checked="" type="checkbox"/>
Display IPV6 addresses:	<input type="checkbox"/>
Enable Zeroconf broadcast:	<input checked="" type="checkbox"/>
Enable log display server:	<input checked="" type="checkbox"/>
Enable clipboard display server:	<input checked="" type="checkbox"/>
Prevent standby while running:	<input checked="" type="checkbox"/>
Select data logging mode:	SSH Server Debug 0

Uočite da s po jednim tapom možemo isključiti web usluge ako nam ne trebaju, time ujedno rasterećujemo RAM i CPU. Uglavnom nam se isplati uključiti opciju za podizanje servisa nakon reboota uređaja – Run SSHelper service at boot.

Tijekom instalacije generiraju se verifikacijski ključevi u formatima RSA, ECDSA i DSA, u konačnici o klijentu ovisi kojim će se ključem odn. enkripcijskim algoritmom štititi konekcija. Najsigurniji je RSA pa je mudro rabiti klijentski softver koji njega preferira.



Očekivano, SSHelper omogućuje tzv. passwordless login pomoću asinkronih ključeva, znači, pogodan je za razne over-the-internet scenarije. Postupak prijelaza na public key autentikaciju naći ćemo u lokalnom helpu, ne moramo se prisjećati ili tragati po Internetu za primjerima kako to odraditi. Zgodno je u ovom kontekstu spomenuti da autentikacija lozinkom, posebno ako je ta lozinka ekstradugačka i kompleksna, nije toliko loša kakvom se često smatra, jer do etape autentikacije dolazi nakon uspostave sesije enkriptirane simetričnim ključem, potom SSH rabi svoj secure password authentication protocol kojim tijekom transporta do servera dodatno štiti unesenu lozinku. Ipak, kad sve saberemo/oduzmemo, autentikacija javnim ključem je sigurnija.

Android uređaj redovito dobija IP parametre od DHCP servisa. Budući da instalacijom SSHelpa taj uređaj de facto postaje server, mudro je osigurati mu permanentnu IP adresu. Ako želimo ostati na DHCP-u, na tom servisu napravimo rezervaciju uparivanjem određene IP adrese sa MAC adresom WiFi kartice. MAC adresu možemo naći na nekoliko mjesta, jedno od njih je Settings > About device. Opcija je postavljanje statičkih IP parametara, što je lako obaviti. Recimo da uređaju sa Lollipop AOS-om želimo postaviti statičke IP parametre: dugački tap na imenu mreže na koju se želimo spojiti > Show advanced options > pod IP settings biramo Static pa unosimo potrebne parametre. Ako se uređaj od ranije automatski spaja na mrežu, čime nam onemogućuje opisani zahvat, prvo se poslužimo naredbom Forget network. Jasno, ta IP adresa ne smije biti u opsegu adresa DHCP servera.

HOMENet



Show advanced options

Proxy

None

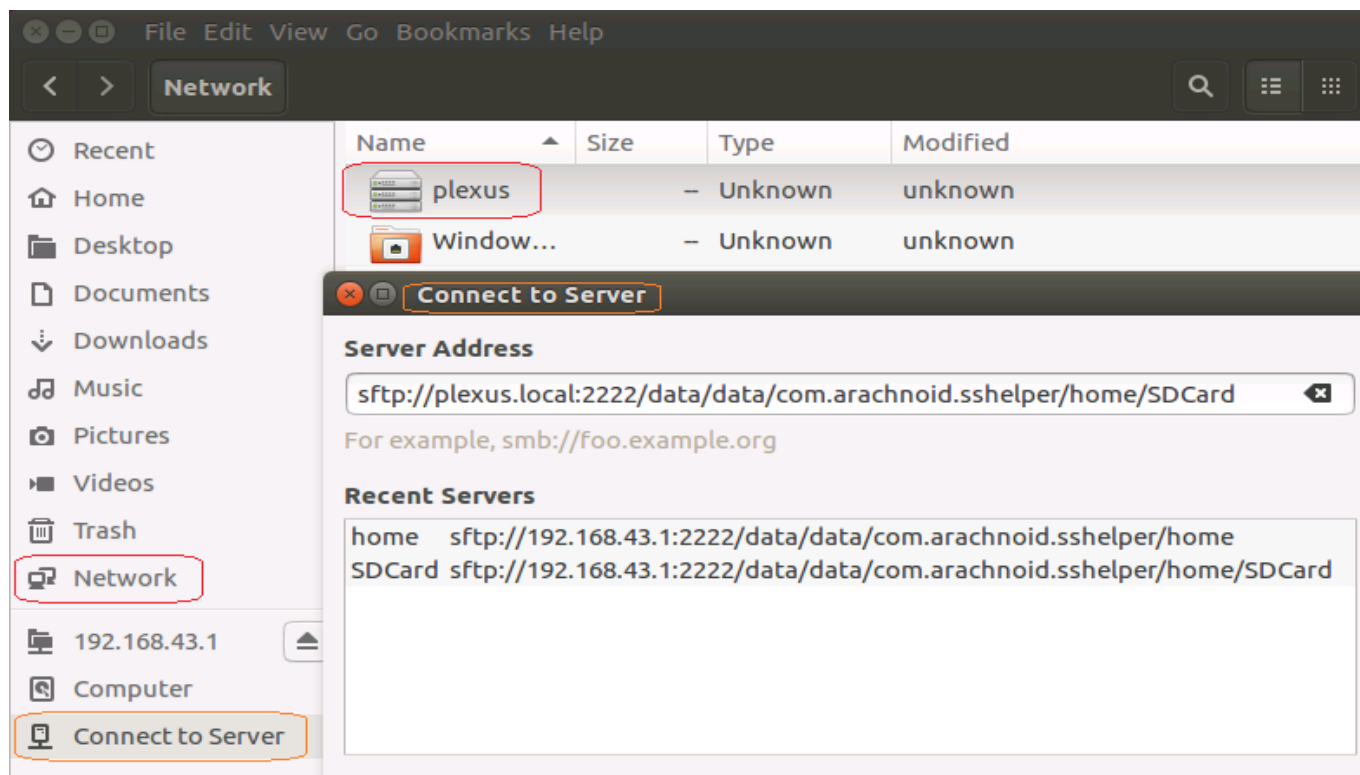
IP settings

DHCP

Static

Glede uporabe imena umjesto IP adrese - zgodno je što se SSHelper na lokalnoj mreži oglašava Java implementacijom Zeroconfig/Bonjour protokola za resolving mrežnih imena pa se na njega možemo spojiti tako da u naredbi (ssh, scp, sftp...) navedemo ime uređaja sa sufiksom local, npr. plexus.local, što je očigledno na trećoj slici ovog članka. Doduše, ovo će proći samo kad su i SSHelper i admin stanica u istoj broadcast domeni, a admin računalo razumije taj protokol. S druge strane, uvijek možemo na klijentskom računalu rabiti lokalnu Hosts datoteku ili čak DNS ako postoji..., vidimo da konačno rješenje ovisi o značajkama mrežne infrastrukture.

Na kraju i par riječi o klijentima. Za početak, dobro je znati da SSH servis odbija SSH-1 tip konekcije, u to se možemo uvjeriti naredbom `ssh -1 -p 2222 ime@IP-SSH-hosta`. Nadalje, kako bismo tijekom SSH sesije nesmetano rabili naredbe SSHelperovog Busyboxa, editirat ćemo datoteku `.profile` (eno je u Home direktoriju SSHelpera) tako da u sekciju „user customizations“ upišemo put kojime favoriziramo BusyBox naredbe. Stvarno korisno na rootanom SSH hostu jer možemo šetkati po njegovim particijama i direktorijima te pozivati potrebnu nam naredbu bez navođenja putanje do nje. `PATH=/data/data/com.arachnoid.sshhelper/bin:/sbin:/system/sbin:/system/bin:/system/sbin`
Ako SSHelperu pristupamo sa Linux računala, u osnovi ne trebamo nikakav dodatni softver. Tu je terminal sa svim potrebnim naredbama a sveprisutni Nautilus možemo iskoristiti na dva načina, niža slika sve objašnjava. Android SSH server je vidljiv na mreži jer i SSHelper i Ubuntu podržavaju ranije spomenuti Zeroconf/Bonjour protokol.



Windows kao SSH klijent? Uz legendarne Putty i WinScp – problema nema! Ako još aktiviramo Windows Subsystem for Linux, prisutan na Desetki, dobijamo i kompletnu komandnu ljusku Ubuntu 16.04 pa možemo „šarati“ kako nam drago.

Kvalitetan klijentski softver postoji i za AOS. Od komandnolinijskih SSH alata poput ConnectBot i JuiceSSH (instalirajte si Hacker's Keyboard!) do GUI aplikacija za scp / sftp / rsync tipove konekcija poput andFTP i ES File Explorer. Završna slika ovog članka pokazuje kako je andFTP iskorišten za sinkronizaciju sadržaja direktorija Docs između dva Android uređaja.

FTP server settings

Hostname: 192.168.43.1

Type: SFTP (SSH File Transfer Protocol)

Port: 2222

Username: ratko

Password: ••••••••

Local dir: /storage/emulated/0

browse

Remote dir: SDCard

Resume: ☒ Enable resume support

Sync type: Mirror remote (Master is remote folder)

Local dir: /storage/emulated/0/DOCS

browse

Remote dir: SDCard/DOCS

Subfolders: ☐ Include (recursive)

Orphan: ☒ Delete discrepancies

Network: ☐ WiFi only

Schedule: Every hour

uto, 2016-08-23 09:11 - Ratko ŽižekKuharice: [Android](#) [1]

Kategorije: [Servisi](#) [2]

Vote: 0

No votes yet

Source URL: <https://sysportal.carnet.hr/node/1672>

Links

[1] <https://sysportal.carnet.hr/taxonomy/term/64>

[2] <https://sysportal.carnet.hr/taxonomy/term/28>