Setup za reverzanje i emuliranje S7-1200

Napomena: Testirano na Fedora 39 OS-u, x86_64 arhitekturi

Upute za Ghidra klijentksu aplikaciju, Ghidra server i itegraciju s Eclipse IDEom

Upute za instalaciju Ghidra SRE na Linuxu

Nulti način - službene upute

https://htmlpreview.github.io/?https://github.com/NationalSecurityAgency/ghidra/blob/Ghidra_11.0.2_build/GhidraDocs/InstallationGuide.html

Prvi način - Flatpak

Najlakši način za instalaciju Ghidre je putem Flatpaka. Flatpak je alat za instalaciju paketa neovisan o Linux distribuciji.
Flatpak upute za pojedine distribucije: https://flatpak.org/setup/
Instalacija Ghidre putem Flatpaka: https://flathub.org/apps/org.ghidra_sre.Ghidra
Ova metoda je jednostavna, ali zbog načina na koji Flatpak instalira aplikacije, Ghidra se neće moći integrirati s Eclipse IDEom za pisanje skripti, pa razmislite je li to nešto što vam treba.

Drugi način - ručno

Prije početka, potrebno je imati instaliranu Javu 17 ili novije (testirano na Javi 21).
Npr:

```
$ sudo dnf install java-17-openjdk
$ sudo dnf install java-17-openjdk-devel
```

Preuzeti najnoviji `ghidra_<ver>_PUBLIC_<date>.zip` s GitHuba:
https://github.com/NationalSecurityAgency/ghidra/releases
Raspakirajte arhivu te sadržaj kopirajte u direktorij gdje u direktorij gdje želite svoju Ghidra instalaciju, npr. u `~/.local/share/ghidra`:

```
$ mkdir -p ~/.local/share/ghidra
$ unzip ghidra_11.0.2_PUBLIC_20240326.zip
$ cp -r ghidra_11.0.2_PUBLIC/* ~/.local/share/ghidra
```

U raspakiranom Ghidra direktoriju nalazi se datoteka `ghidraRun` kojom se aplikacija može pokrenuti:

```
$ cd ~/.local/share/ghidra
$ ./ghidraRun
```

Prvi put pokušajte pokrenuti ovako da se uvjerite da Ghidra nalazi Javu. Ako se pokrene dialog za unos Java direktorija, unesite sljedeću (ili neku sličnu) putanju: `/usr/lib/jvm/jdk-21-oracle-x64/bin/`.

Zbog jednostavnosti, željeli bi da se Ghidra može pokrenuti i putem GUI-a. Stvorite datoteku `ghidra.desktop` u direktoriju `~/.local/share/appliactions` te u nju kopirajte:

```
[Desktop Entry]
Name=Ghidra
Comment=SRE Suite
Exec=/home/<user>/.local/share/ghidra/ghidraRun
Icon=ghidra
Type=Application
Path=/home/<user>/.local/share/ghidra/
```

Prilagodite putanje po potrebi. Testirano na Gnomeu, a trebalo bi raditi i na KDE, xfce okolinama.
Ako se ikona ne pojavljuje među ostalim aplikacijama, pokušajte na neki način resetirati GUI sjednicu (npr. logout/login).

Upute za pristup projektu na Ghidra serveru

Na meniju odabrati opciju *File > New project* te odabrati *Shared Project* za tip projekta.
Unijeti IP/DNS ime servera (ghidra.zemris.fer.hr u ovom slučaju) te ostaviti defaultni port 13100.
Nakon prijave, odaberite željeni projekt. Pri prvom otvaranju projekta treba se odabrati lokacija na lokalnom računalu gdje će se spremati potrebne datoteke. Preporučujem negdje stvoriti zasebi direktorij za ovo, npr. `ghdira_projects`.
Dalje je korištenje Ghidre *business as usual* (ako se samo čitaju datoteke, kontrola verzija pri mjenjanju sadržaja datoteka će, po potrebi, biti posebno pokrivena tutorialom).

Upute za postavljanje Ghidra servera

Najjednostavnije s pomoću Dockera.
Upute za instalaciju Dockera: https://docs.docker.com/engine/install/
Docker image i upute za pokretanje: https://hub.docker.com/r/bytehow/ghidra-server
Osnovno o Ghidra serveru: https://byte.how/posts/collaborative-reverse-engineering/

Upute za Ghidra scripting

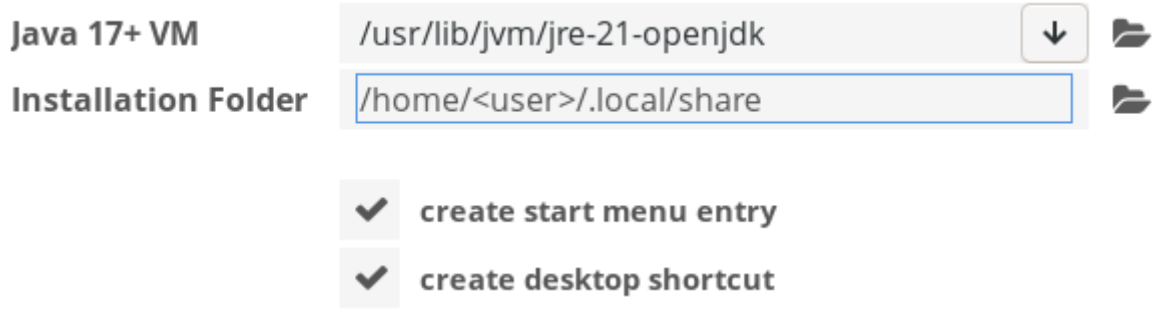
Ghidra ima mogućnost pisanja skripti u Javi ili Pythonu. Ghidra skripte su programi koji se mogu koristiti za automatiziranje radnji koje bi inače radili ručno. Ghidra pruža uređivač teksta za pisanje ovih programa, ali za veće programe je potrebno imati bolji IDE. Ghidra nudi mogučnost integracije sa Eclipse IDEom.

Upute za instalaciju Eclipse IDEa

Preuzeti instaler sa https://www.eclipse.org/downloads/packages/
U terminalu navigirati do preuzete datoteke.
Zatim:

```
# raspakirati
$ tar -xvf eclipse-inst-jre-linux64.tar.gz

# pokrenuti instalaciju
$ cd eclipse-installer
$ ./eclipse-inst
```

Odabrati `Eclipse IDE for Java Developers`.
Za `Instalation foler postaviti` direktorij `./local/share` (ili gdje već držite instalacije), a ostale checkboxeve ostaviti.



Nakon ovog, Eclipse IDE bi se trebao pojaviti s ostalim aplikacijama.
Iz nekog razloga, Eclipse instaler stvori dvije `.desktop` datoteke (`eclipse.desktop` i `epp.package.java.desktop`) pa sustav pokazuje dvije Eclipse ikone, ali one zapravo pokreću istu aplikaciju:

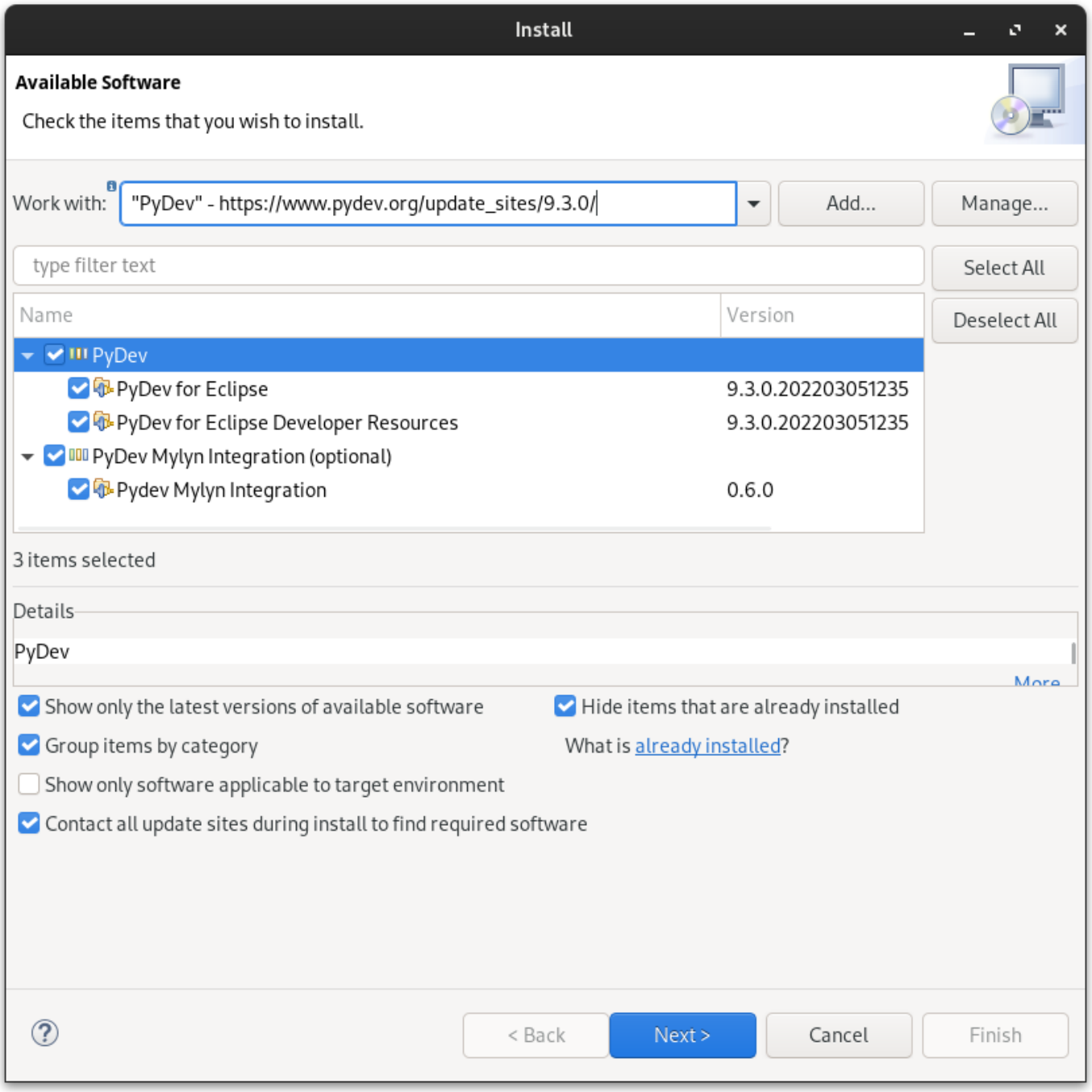
Ako vam je ovo problem, obrišite jednu od tih datoteka:

```
$ cd ~/.local/share/applications
$ ls -l | grep eclipse
$ cat epp.package.java.desktop
[Desktop Entry]
Type=Application
```

```
Terminal=false
Encoding=UTF-8
Version=1.1
Name=Eclipse IDE for Java Developers - 2024-03
StartupWMClass=Eclipse
Exec=/home/<user>/.local/share/eclipse/eclipse
Categories=Development;IDE;Eclipse
Icon=/home/<user>/.local/share/eclipse/icon.xpm
$ rm epp.package.java.desktop
```

Priprema Eclipse IDE-a za integraciju s Ghidrom

Potrebno je instalirati PyDev plugin za Eclipse. Ghidra integracija ne radi sa novijim verzijama PyDev plugina (12 u vrijeme pisanja), a najnovija koja radi je verzija 9.3.
Popis svih PyDev verzija: https://www.pydev.org/update_sites/
U Eclipseu odabrati `Help > Install new software`, te u polje `Work with` upisati poveznicu `https://www.pydev.org/update_sites/9.3.0/` (i stisnuti enter).

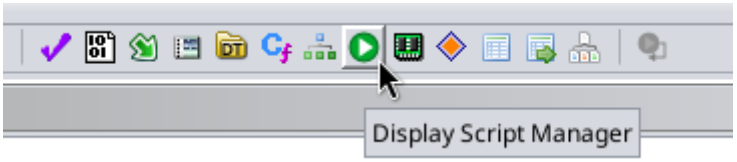


Dalje pratiti instalaciju i pričekati da završi (progress bar u donjem desnom kutu).
Za dodatnu provjeru je li instalacija prošla uredu, provjerite `Window > Perspective > Open Perspective > Other`.

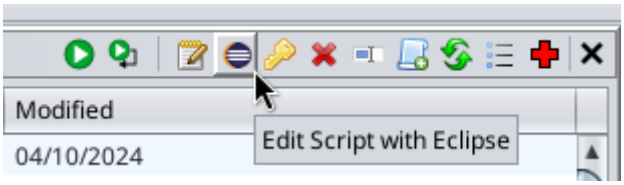
Potrebno je instalirati i GhidraDev plugin za Eclipse. Arhiva koja sadrži taj plugin se nalazi u instalacijskom direktoriju Ghidre.
U Eclipseu odabrati `Help > Install new software > Add... > Archive...`, te navigirajte to `<ghidra install>/Extensions/Eclipse/GhidraDev/GhidraDev-3.0.2.zip`
Pratite instalaciju. Kada je gotova, GhidraDev će se pojaviti kao opcija na alatnoj traci.

Integracija s Ghidrom

Otvorite Ghidru i u njoj neki projekt i datoteku. Otvorite *Script Manager*:



U *Script Manageru* odaberite neku skriptu s liste, npr. `HelloWorldScript.java`.
Dvoklikom na skriptu će se ona izvesti te se ispis može vidjeti u konzoli *Code Browsera*.
Za otvaranje skripte u Eclipseu kliknite Eclipse ikonu u gornjem lijevom kutu:



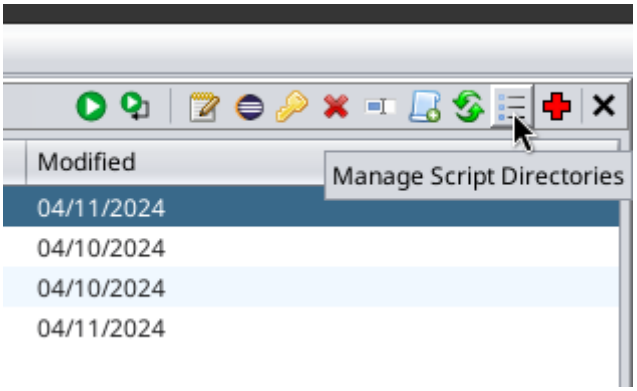
Pri prvom otvaranju, Ghidra će tražiti da unesete instalacijski direktorij Eclipsea (u slučaju ovih uputa: `/home/<user>/.local/share/eclipse`).
Također, po potrebi će ponuditi dialog za stvaranje novog Ghidra Scripting projekta.
Pri dodavanju novog projekta, Eclipse će se pokušati povezati sa Ghidra instalacijom i sa skriptama u `/home/<user>/ghidra_scripts` direktoriju (ovo ne želimo jer taj direktorij vjerojatno ne postoji i ne želimo ga stvoriti). Za dodavanje Ghidra instalacije, potrebno je reći Eclipseu gdje Ghidra instalacijski direktorij (`/home/<user>/.local/share/eclipse`). Eclipse će također opcionalno tražiti Jython interpreter (ne zahtjeva posebnu instalaciju, dolazi sa Ghidrom), kojeg će automatski pronaći u Ghudrinom instalacijskom direktoriju.
Sada kad je sve postavljeno, klik na Eclipse ikonu će otvarati odabranu skriptu u Eclipseu.

Ghidra instalacija dolazi s velikim brojem gotovih skripti koje se mogu pronaći u `<ghidra install>/Ghidra/Features/Base/ghidra_scripts`. Također se mogu pronaći u Eclipseu kad se otvori Ghidra projekt sa lijeve strane prozora, u *Package Exploreru*, iako nisu u samom direktoriju projekta, čak ni kao simbolički linkovi.
Za nove skripte je poželjno stvoriti novi *Source Folder* desnim klikom u *Package Exploreru* na `<package name> > New > Source Folder` te stvoriti ga u korijenu projekta, nazvati ga npr. *LocalScripts*. Ovaj direktorij će se stvoriti u direktoriju projekta, zajedno sa svim skriptama u njemu (za razliku od skripti s kojima Ghidra dolazi).
Nove skripte mogu se dodavati pomoću GhidraDeva u alatnoj traci: `GhidraDev > New > Ghidra Script...`. Za kratku testnu skriptu možete napisati:

```
//Hello world to test adding scripts to Ghidra

import ghidra.app.script.GhidraScript;

public class MyHelloWorld extends GhidraScript {

    @Override
    protected void run() throws Exception {
        println("My local hello world.");
    }
}
```

(Ne zaboravite *Ctrl* + *S*)

Ghidra po defaultu ne učitava nove skripte. Za to je potrebno sljedeće:



U ovom prozoru treba dodati novi direktorij, tj. novi projekt sa skriptama koje radimo klikom na zeleni plus (gore desno u prozoru). Nakon toga je potrebno i osvježiti te direktorije (gore desno u prozoru). Nakon toga tek možemo vidjeti nove skripte u popisu u *Script Manageru*.