Interview Protocol

[Overarching Question]

How do different lockfile features affect the developer experience?

[Introduction]

We are conducting a study on dependency management, comparing the developer experience on lockfiles across different package managers.

[Wait for a moment for any replies, and let them introduce themselves before continuing]

We are here to understand the experience of open-source software developers in managing their dependencies with and without lockfiles. As we mentioned in our previous email, we came across your GitHub project <project name> and we would love to discuss your experience on managing third-party dependencies of your project. This interview will take about 20 minutes, during which time **we'll go through some questions regarding lockfiles and common dependency management processes you follow**. Do you have any questions for me so far?

A couple of things before we start. As we have mentioned in the consent form, which we sent earlier by email, to the extent possible, we will take your comments to be **confidential**. We will aggregate all the comments from the eight interviews we're conducting so that your comments are not traced to you. If we quote you in our paper, we will do so without identifying your name or specific role. If there's anything you really don't want us to report, even if it's anonymized, please let me know that, too. Also, this interview is entirely **voluntary** on your part – if for any reason you want to stop, please let us know. We can end the interview at that point with no repercussions for you of any kind. If you wish, we can also throw out my notes of what you've told me until that point.

Do you have any questions for me? All right, then, let's proceed.

[Once the interview gets underway…] Oh, and by the way, do you mind if I **record** this call? This is just so that my team doesn't miss anything – no one except for the core research team will have access to the recording. Thanks.

[Warm up / Background]

(Common for both Case 1 and Case 2)

For how long have you been a software developer?

In which areas have you been working?

How long have you been using the <package manager> as a <language> developer?

Case 1

[Prepping for the interview]

What reasons led you to choose <package manager> over other package managers?

Do you normally commit lockfiles in all of your <package manager> projects?

Have you ever faced any issues related to dependencies such as version conflicts or breaking updates?

How do you solve them?

According to your experience, what kind of benefits does the usage of <package manager> lockfiles provide compared to not using a lockfile?

[Semi-structured interview questions]

Do you manually check the lockfile content once it is created? Why?

Do you use it as a debugging technique? Why?

Do you see any security advantage in committing the lockfile?

What are they?

Do you manually check the lockfile content?

When and why?

Do you check this during code reviews? Why?

When you do that, which information is included in the lockfile do you find most useful?

Do you manually edit the lockfile?

When do you do that?

At which times do you commit lockfiles in the project after the initial commit?

Do you commit it in every PR?

[if yes] how do you resolve merge conflicts

[if no] when do you commit?

Do you normally enforce the lockfile when you build the project? Why?

[If yes and did not mention a specific phase] When do you think it becomes useful?

[If they mention ci/cd pipelines ask more about it.]

Do you use any other tools to ensure the integrity of downloaded packages or to achieve deterministic builds?

What functions do you normally use with lockfiles?

Do those commands always work as you expect?

[A clarification] Have you ever run into any difficulties in fulfilling your requirements?

[If there is time, and if the answer is interesting] Can you explain a bit more about one such issue you faced and how you resolved it?

In what ways do you think the lockfile feature could be improved?

Do you have any other thoughts that you would like to share with us?

Case 2

[Prepping for the interview]

What reasons led you to choose <package manager> over other package managers?

Have you ever faced any issues related to dependencies such as version conflicts or breaking updates?

How do you solve them?

Do you normally use lockfiles with your other projects?

What reasons led you to not commit lockfiles in this project?

[Semi-structured interview questions]

What were the reasons for not committing lockfiles in your projects?

Even though you don't commit the lockfile,

Do you refer to it locally as it gets generated automatically when you build? Why?

Do you use any <package manager> commands related to lockfiles using the locally generated lockfile? Why?

How do you track the transitive dependencies of your project?

What is your approach to reviewing the dependencies during code reviews?

Do you use any other tools

to ensure the integrity of downloaded packages?

to achieve deterministic builds?

[if they use lockfiles locally] What are the challenges that you face when using lockfiles?

[if not] What are the challenges that you face when managing dependencies?

In what ways do you think the lockfiles can be improved?

Do you have any other thoughts that you would like to share with us?

[Conclusion]

Those are all the questions we have for you. If anything else occurs to you later, please don't hesitate to let us know by email. We may be in touch with you again to ask a few follow-up questions. Thanks a lot for sharing your opinions with us today. And, in about 6 weeks, after we've concluded all the interviews and our analysis, we will send you our final report. Thanks again!