V8 Pwn Cheat Sheet

V8 version

```
commit d8914f7033295aa02fa72a73344e84edff87c70a (HEAD, tag: 10.5.118,
origin/chromium/5159, origin/chromium/5158, origin/chromium/5157, origin/canary,
origin/10.5.118)
Author: v8-ci-autoroll-builder <v8-ci-autoroll-builder@chops-service-
accounts.iam.gserviceaccount.com>
Date:   Fri Jul 1 11:01:06 2022 -0700

    Version 10.5.118

    Change-Id: I7d0574b460ea4c42ede4227d2ad3cd27f461b23b
    Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/3740713
    Bot-Commit: v8-ci-autoroll-builder <v8-ci-autoroll-builder@chops-service-
accounts.iam.gserviceaccount.com>
    Cr-Commit-Position: refs/heads/10.5.118@{#1}
    Cr-Branched-From: db3e14d3a231a1cf9eec888cf0a950aecf4a6d0b-
refs/heads/main@{#81497}
```

Map

- Map, map.tq
  - DescriptorArray
    - `details` may be encoded `field_index` and `representation`
      - PropertyDetails
    - `value` may be `Weak<Map>`

Objects

- Object
  - HeapObject
    - JSReceiver
      - JSObject
        - JSArray
        - JSArrayBuffer
          - `backing_store` is `RawPtr`

Inline Cache

- IC
  - FeedbackNexus
    - FeedbackVector
      - TorqueGeneratedFeedbackVector

Prototype Chain

- LookupIterator::LookupIterator
  - LookupIterator::GetRoot
  - LookupIterator::GetRootForNonJSReceiver
- LookupIterator::Next
  - LookupIterator::NextInternal
  - LookupIterator::NextHolder
  - update `holder_`

SetNamedProperty

- SetNamedProperty
- InterpreterSetNamedPropertyAssembler::SetNamedProperty
- AccessorAssembler::StoreIC
  - Runtime_StoreIC_Miss
    - StoreIC::Store
    - MigrateDeprecated
      - JSObject::MigrateInstance
      - JSObject::MigrateToMap
      - JSObject::MigrateToMap
      - MigrateFastToSlow
      - transition from deplicated Map
    - Object::SetProperty
      - Object::SetPropertyInternal
        - Object::SetDataProperty
        - Map::PrepareForDataProperty
        - UpdateDescriptorForValue
        - MapUpdater::ReconfigureToDataField
          - MapUpdater::TryReconfigureToDataFieldInplace
            - MapUpdater::GeneralizeField
            - MapUpdater::GeneralizeField
            - MapUpdater::UpdateFieldType
            - DescriptorArray::Replace
            - update Map.value
          - MapUpdater::ConstructNewMap
            - Map::DeprecateTransitionTree
            - deplicate existing Map, and make migrated Map
      - Object::AddDataProperty
        - Object::TransitionAndWriteDataProperty
        - LookupIterator::PrepareTransitionToDataProperty
        - Map::TransitionToDataProperty
          - TransitionsAccessor::SearchTransition
            - use existing Map
          - Map::CopyWithField
            - make new Map

GetNamedProperty

- GetNamedProperty
- AccessorAssembler::LoadIC_BytecodeHandler
  - AccessorAssembler::TryMonomorphicCase
    - CodeStubAssembler::IsWeakReferenceTo
    - lookup handler by `lookup_start_object_map`
  - AccessorAssembler::LoadIC_Noninlined
    - lookup handler by `lookup_start_object_map`
  - Runtime_LoadIC_Miss
    - LoadIC::Load
    - MigrateDeprecated
    - IC::update_lookup_start_object_map
      - `lookup_start_object_map_ = receiver.map`
    - LoadIC::UpdateCaches
    - LoadIC::ComputeHandler
  - AccessorAssembler::HandleLoadICHandlerCase
    - use handler

GetNamedPropertyFromSuper

- GetNamedPropertyFromSuper
- AccessorAssembler::LoadSuperIC
- AccessorAssembler::HandleLoadICHandlerCase