

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.h](#), [map.tq](#)
 - [descriptor-array.tq](#)
 - [PropertyDetails](#)
 - If object has fast mode properties, PropertyDetails contains a property index
 - [AccessInfoFactory::ComputeDataFieldAccessInfo](#)
 - PropertyValue may contains Weak<Map>

Objects

- [objects.h](#)
 - [HeapObject](#)
 - [JSReceiver](#)
 - [JSObject](#)
 - [JSArray](#)
 - [JSArrayBuffer](#)

Inline Cache and Map Transition

- [IC](#)
 - [FeedbackNexus](#)
 - [FeedbackVector](#)
 - [feedback-vector.tq](#)
- [GetNamedProperty](#)

- [AccessorAssembler::LoadIC_BytecodeHandler](#)
 - [Runtime_LoadIC_Miss](#)
- [SetNamedProperty](#)
 - [InterpreterSetNamedPropertyAssembler::SetNamedProperty](#)
 - [AccessorAssembler::StoreIC](#)
 - [Runtime_StoreIC_Miss](#)
 - [StoreIC::Store](#)
 - [MigrateDeprecated](#)
 - [JSObject::MigrateInstance](#)
 - [JSObject::MigrateToMap](#)
 - [JSObject::MigrateFastToSlow](#)
 - [Object::SetProperty](#)
 - [Object::SetPropertyInternal](#)
 - [Object::AddDataProperty](#)
 - [Object::PrepareTransitionToDataProperty](#)