新竹阿婆天天逆向(工程)

terrynini38514

terrynini


ANTI ANALYZE

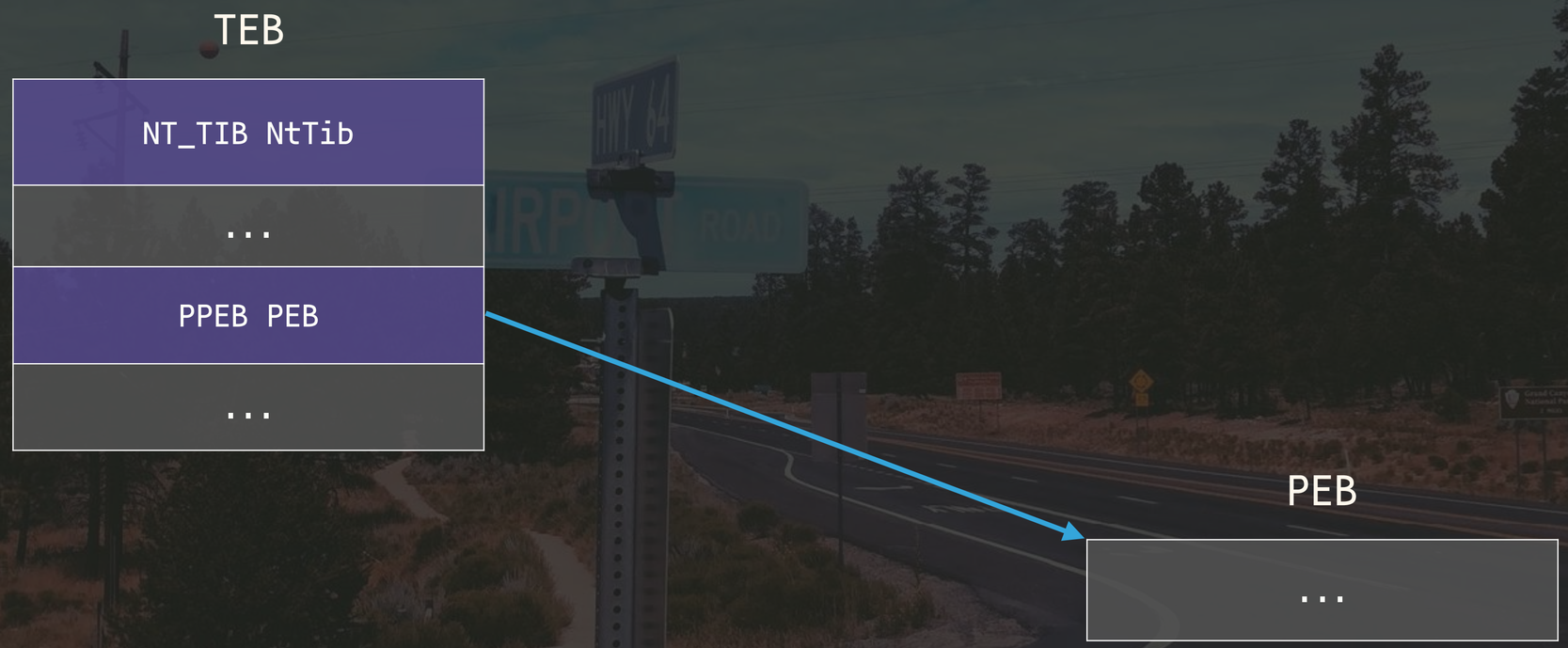
Anti-Analyze

- 對抗分析的方法有許多，包含靜態及動態，基本上就是要增加逆向分析成本
- 各個技巧可能看似簡單，但組合在一起非常崩潰
- 相關技巧非常仰賴作業系統，不同作業系統下會有不同的方法，當然也是有通用的
- 這裡以 Windows 為例，因為 Windows 比較噁心

TEB(Thread Environment Block)

- TEB 用來保存當前執行緒相關的資訊
- 可以透過其中的 TIB 以及 PEB 直接獲得某些資訊而不需要使用 API
- 在 32bit 系統上可以透過 fs 存取
- 在 64bit 系統上可以透過 gs 存取

TEB



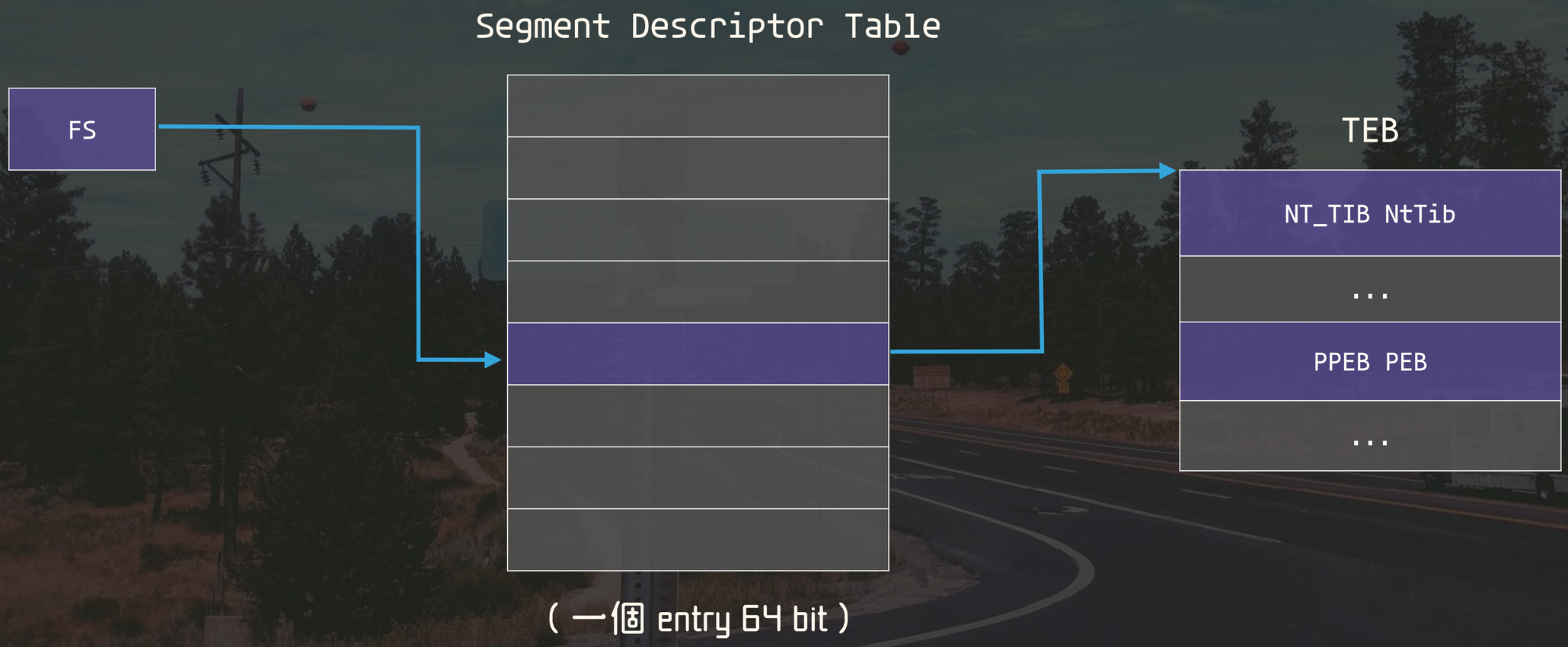
TIB (Thread Infomation Block)

(ProcessEnvironmentBlock太長，member名縮寫)

How To Get TEB

```
Ntdll.NtCurrentTeb()
```

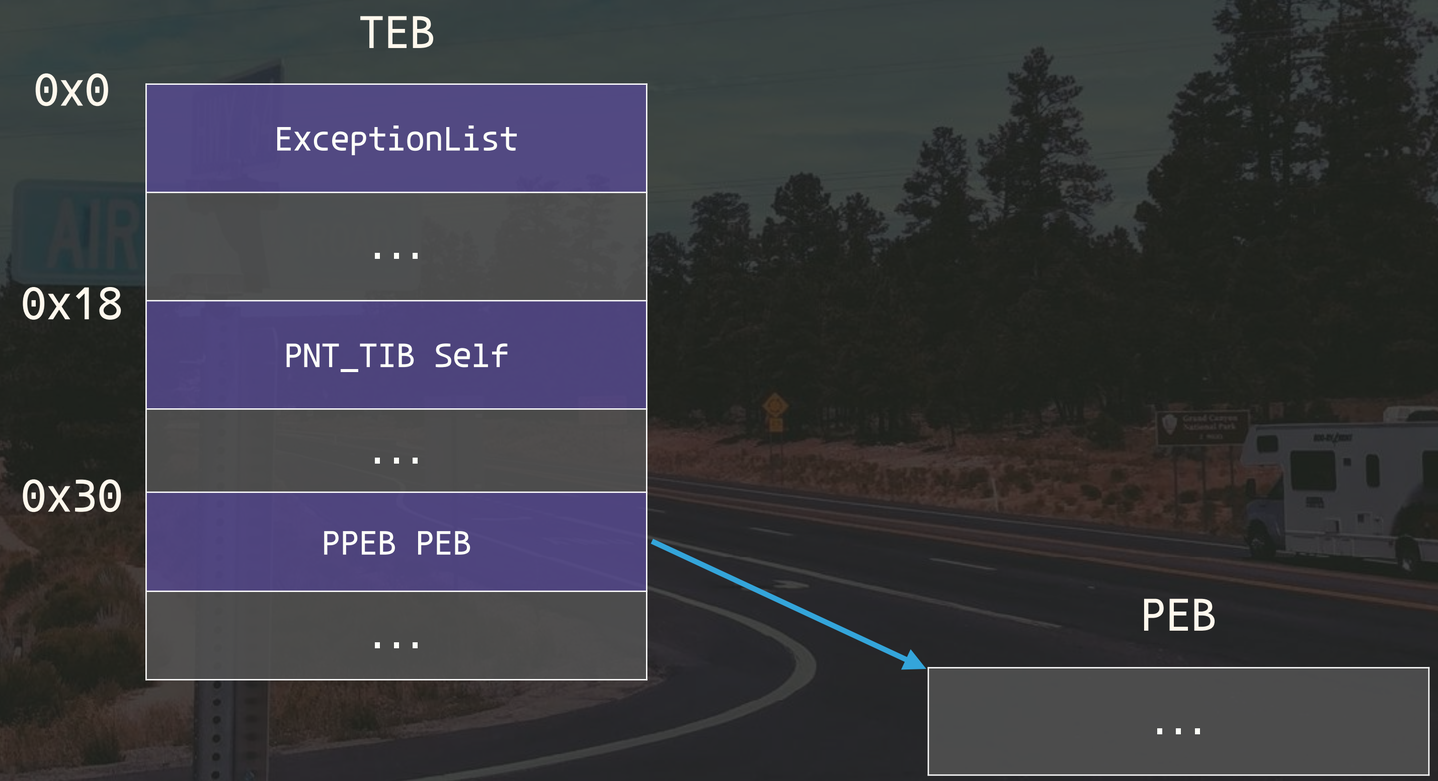
How To Get TEB



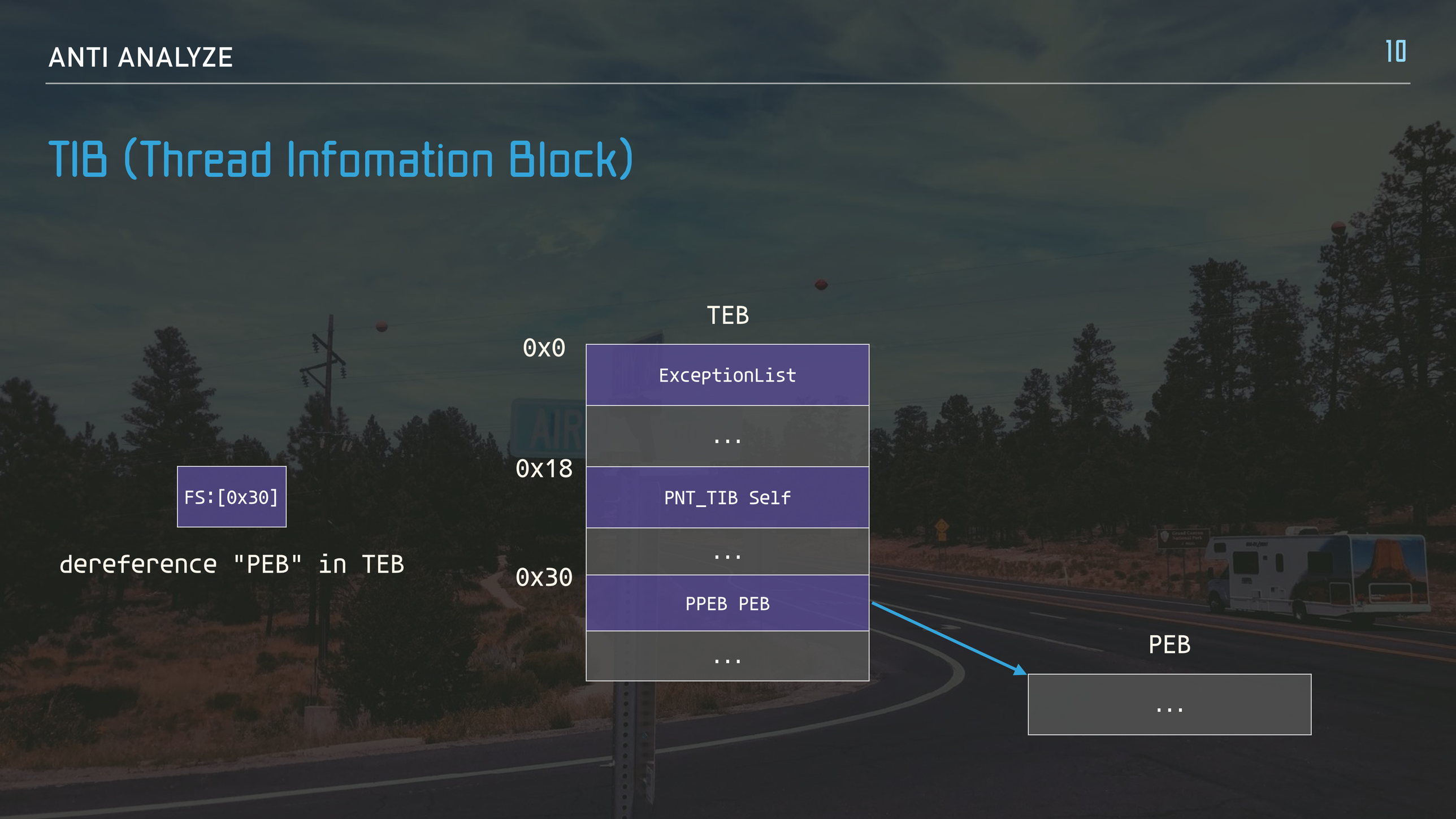
TIB (Thread Infomation Block)

FS:[0x18]

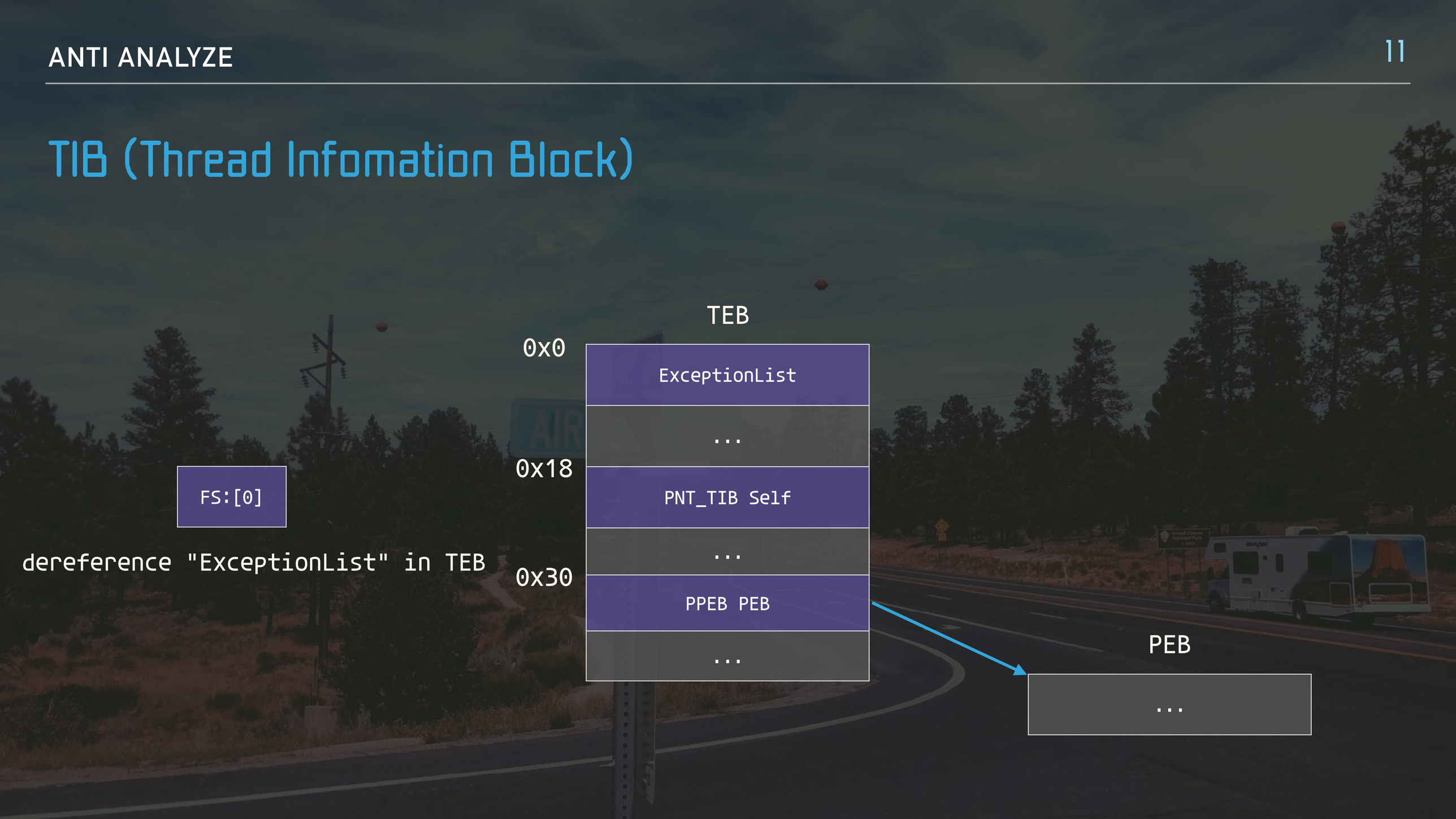
dereference "Self" in TEB



TIB (Thread Infomation Block)



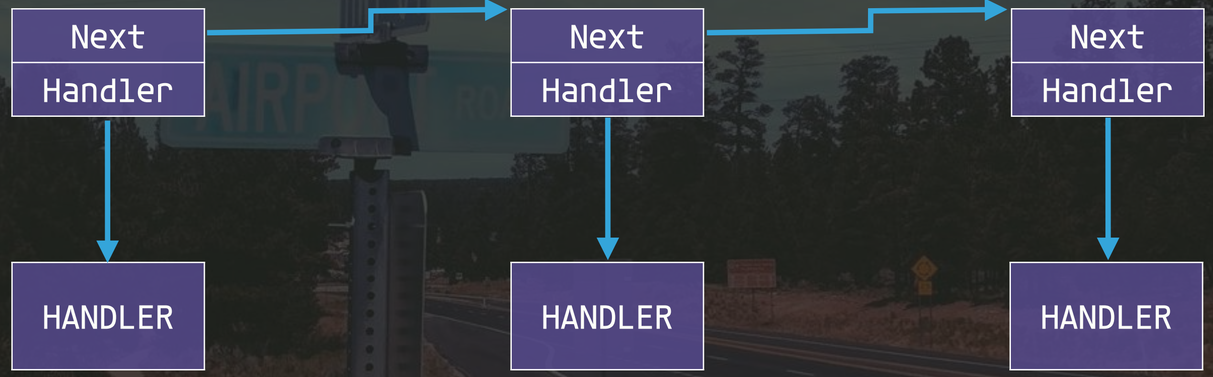
TIB (Thread Infomation Block)



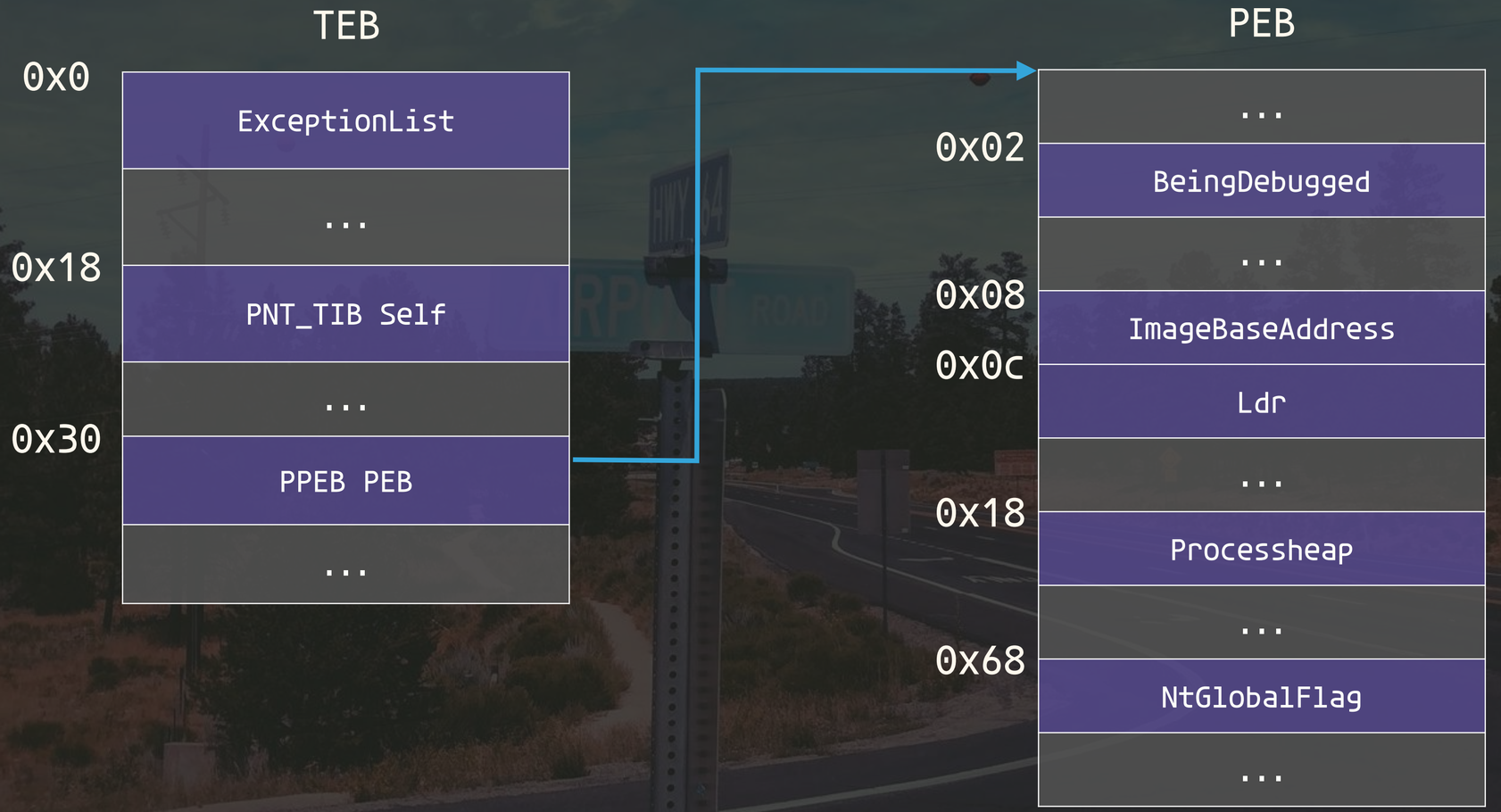
TEB


Exceptionlist
TIB Self
PEB
32bit
FS:[0]
FS:[0x18]
FS:[0x30]
64bit
GS:[0]
GS:[0x30]
GS:[0x60]

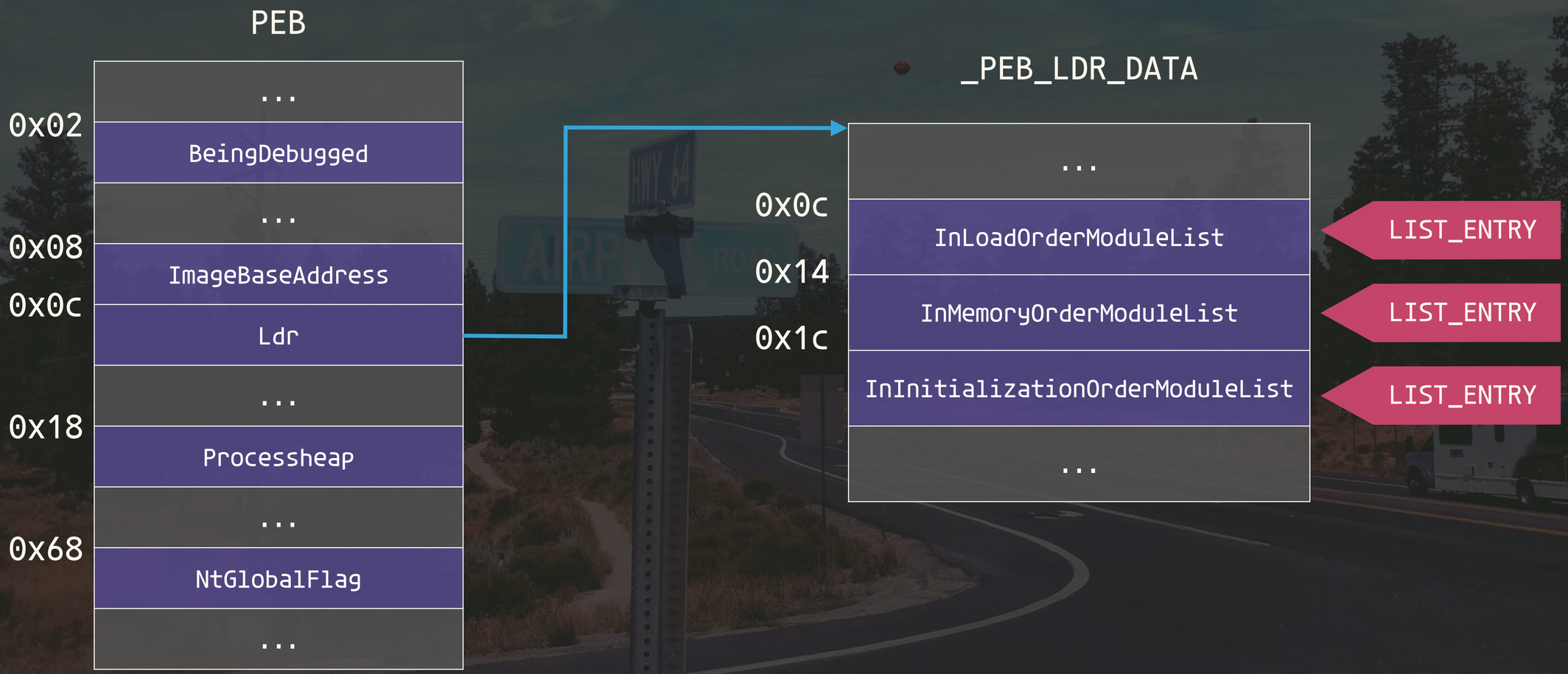
SEH


Next
Handler
HANDLER
Next
Handler
HANDLER
Next
Handler
HANDLER

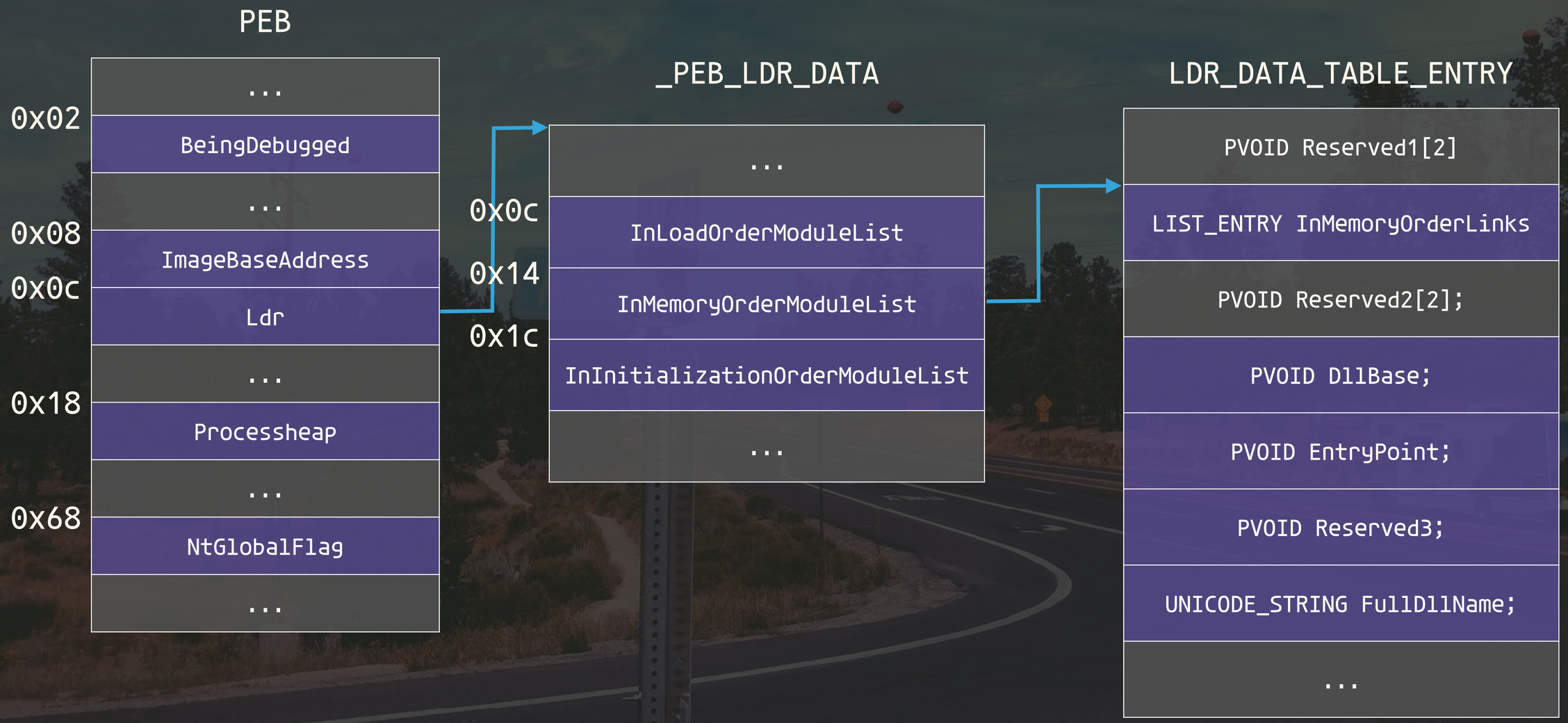
PEB (Process Environment Block, 32bit)



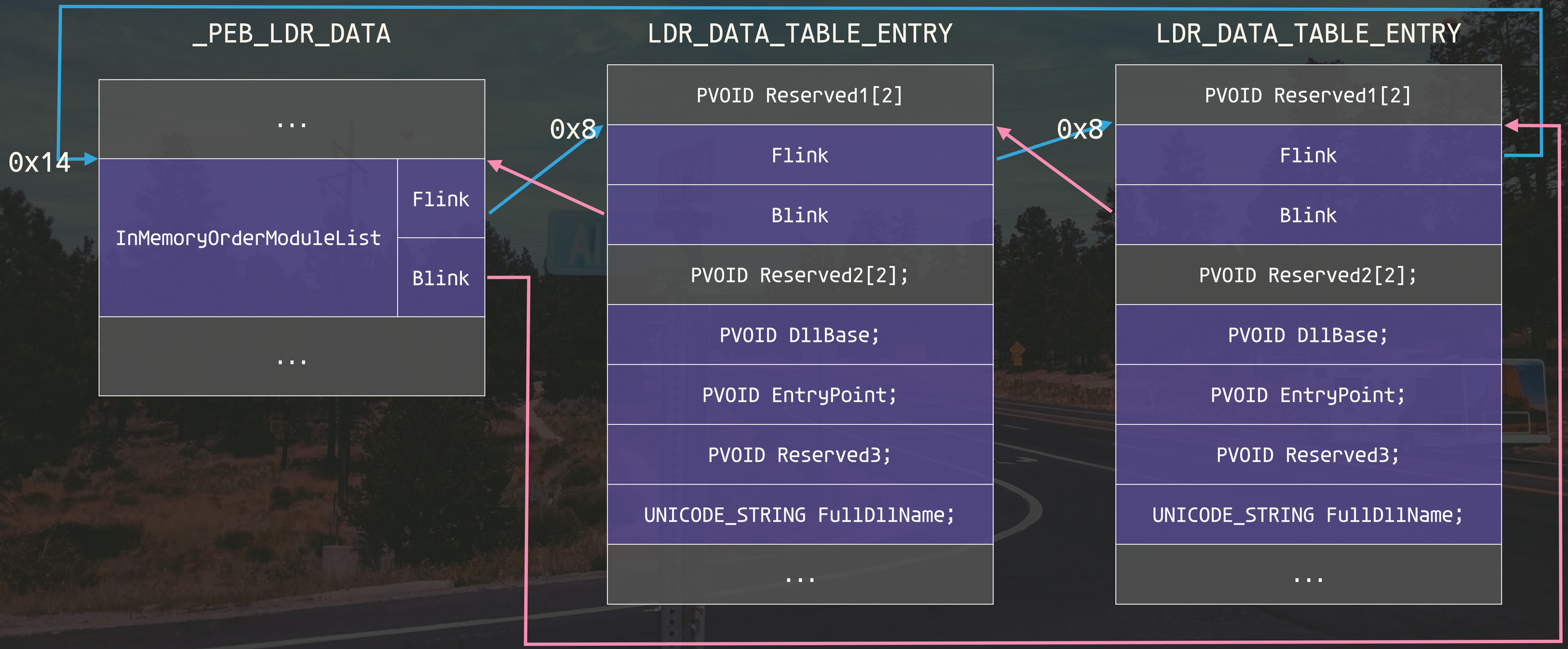
PEB (Process Environment Block, 32bit)



PEB (Process Environment Block, 32bit)



PEB (Process Environment Block, 32bit)



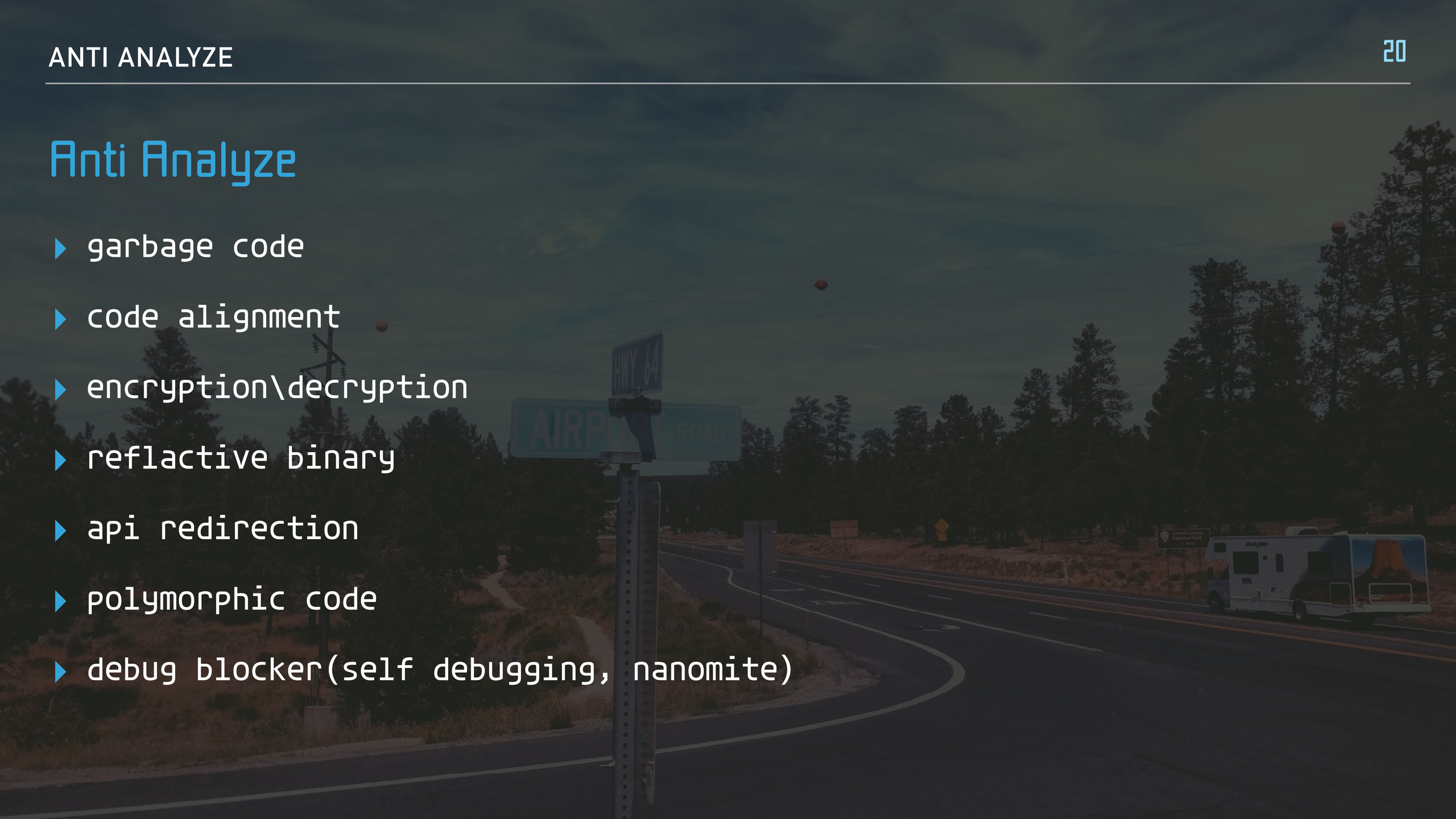
Anti Analyze

- 大家都理解了
  所以現在大家都煉銅
- 煉銅不是不好,
  但我們可以精進一下

DIY

Anti Analyze

- garbage code
- code alignment
- encryption\decryption
- reflactive binary
- api redirection
- polymorphic code
- debug blocker(self debugging, nanomite)



Anti-Analyze

Debugger Detection

- PEB
  - BeingDebugged
  - NtGlobalFlag

Debugger Detection

- NtQueryInformationProcess()
- CheckRemoteDebuggerPresent()
- NtQueryInformationProcess()
- NtQuerySystemInformation()
- NtSetInformationThread()
- NtQueryObject()

Debugger Detection

- FindWindow()
- Parent Process Check()
- GetComputerName()
- GetCommandLine()

END

Reference

- https://ithelp.ithome.com.tw/articles/10219105