Reverse Android malware like a Jedi

Axelle Apvrille, Fortinet

Virus Bulletin Conference, October 2021

Who am I?

Axelle Apvrille, @cryptax

Principal Security Researcher for Mobile Malware and IoT at

FORTINET®

Lead organizer of smart devices CTF

ph0wn

Advanced tools for Android reverse engineering

Dexcalibur - 2019

https://github.com/FrenchYeti/dexcalibur

House

House - 2018

https://github.com/nccgroup/house

MobSF - 2015

https://github.com/MobSF/Mobile-Security-Framework-MobSF

QUARK

Quark - 2019

https://github.com/quark-engine/quark-engine

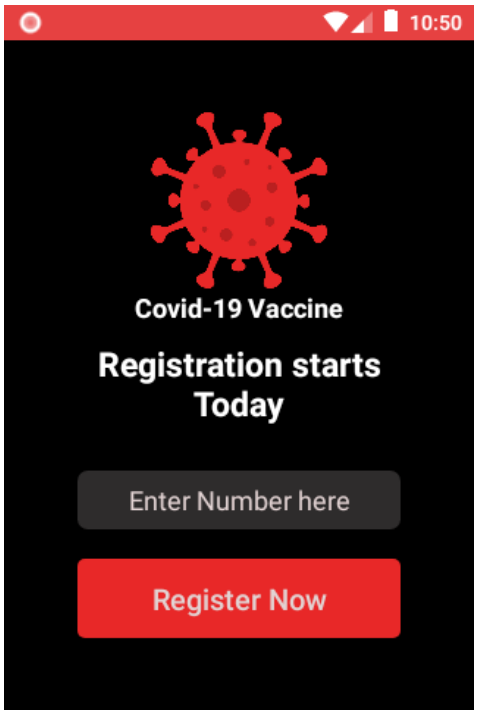
You need this for Dynamic Analysis

Emulator

FRIDA

Frida server `https://github.com/frida/frida/releases/`

and client!



Sample of Android/Oji.G!worm

Malware (APK)

From user point of view...

	Dexcalibur	House	MobSF	Quark
Setup	★	★★	★★★	★★★
Use	★★★	★	★☆	★★☆

personal opinion - all tools are actually awesome!

Which tool? (preferred choices only)

- Unpacking
- Network monitoring
- De-obfuscate
- File or shared prefs monitoring
- General API monitoring
- Bypass debugger / rooting detection
- Specific hook
- Static analysis

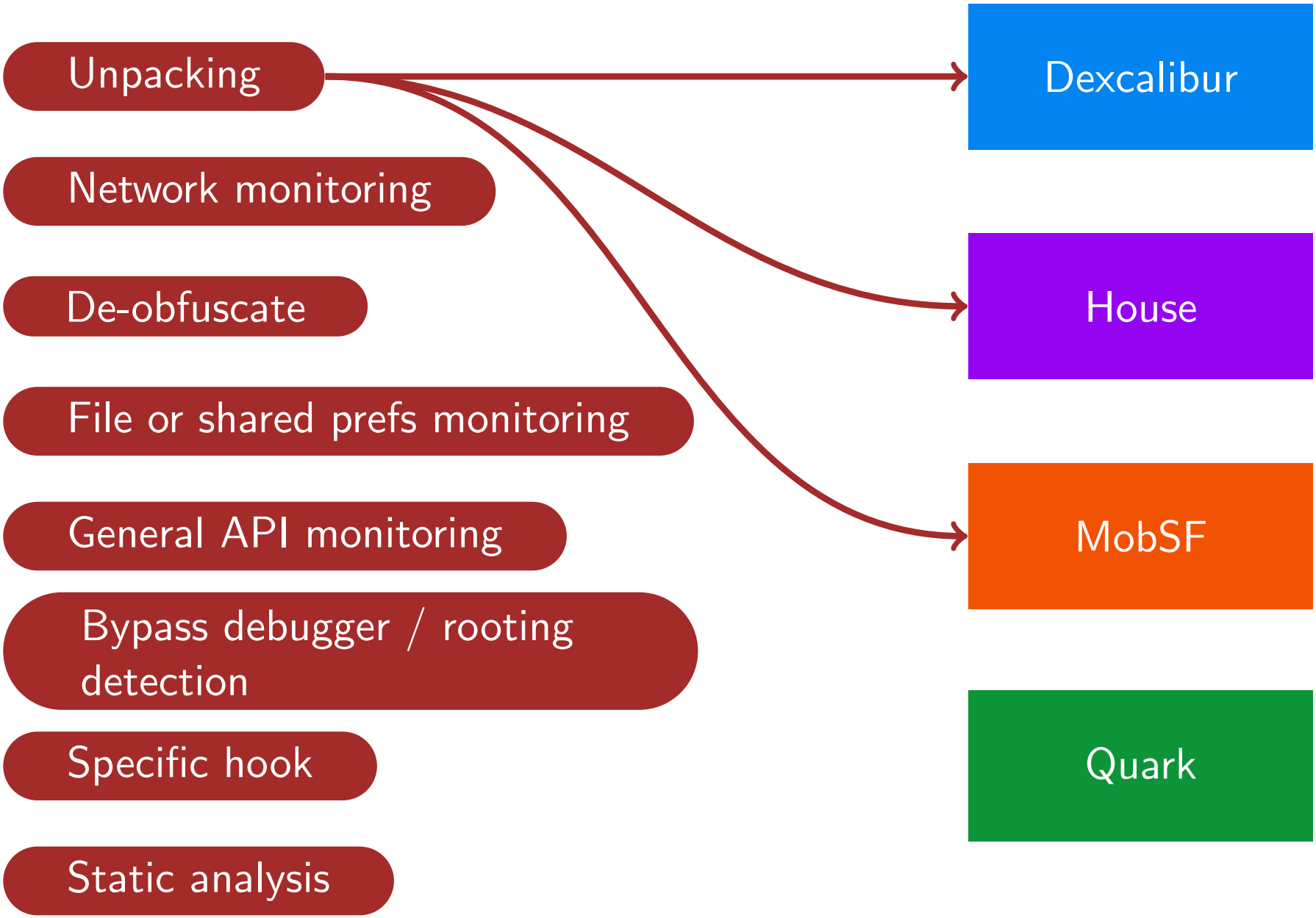
Dexcalibur

House

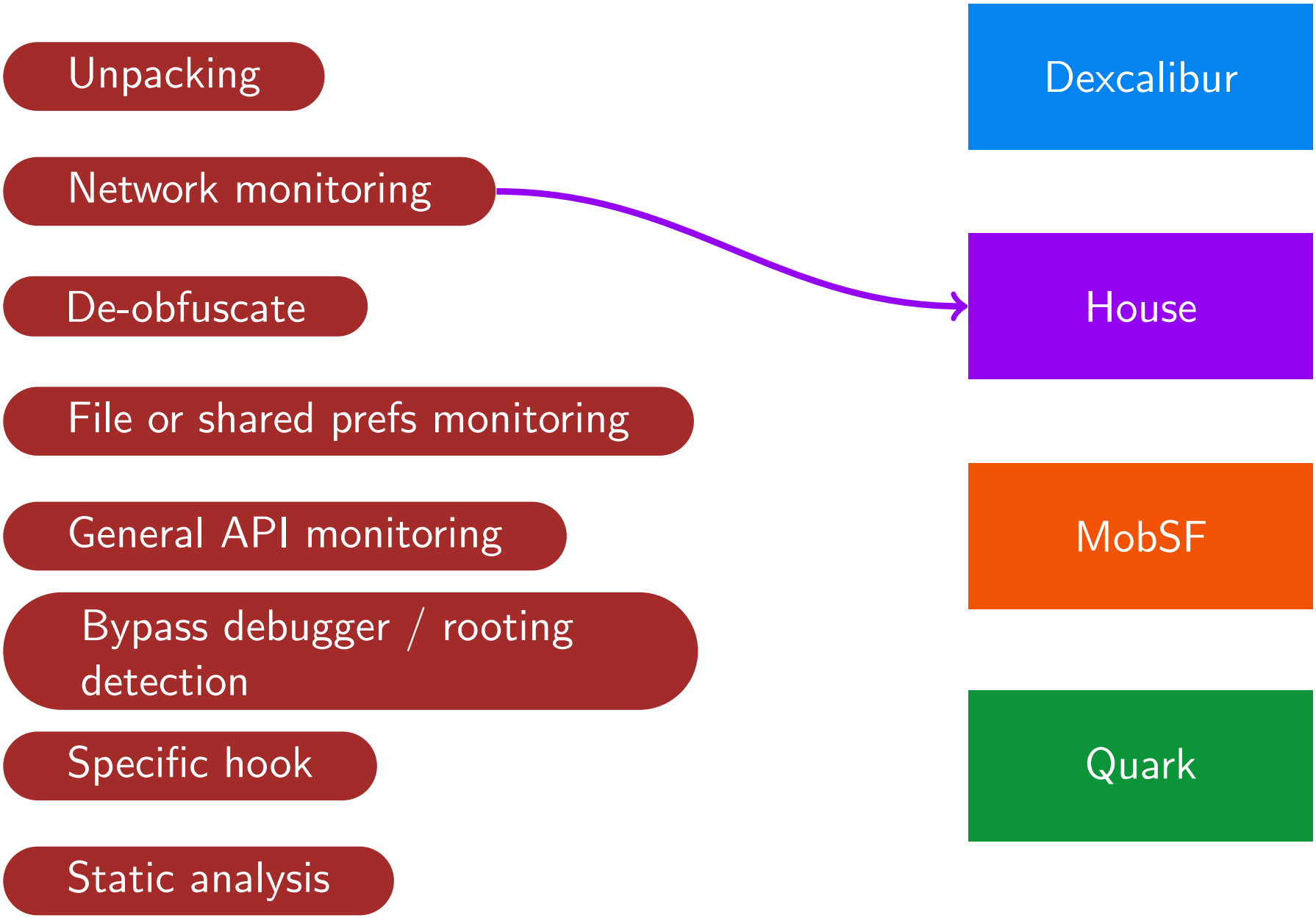
MobSF

Quark

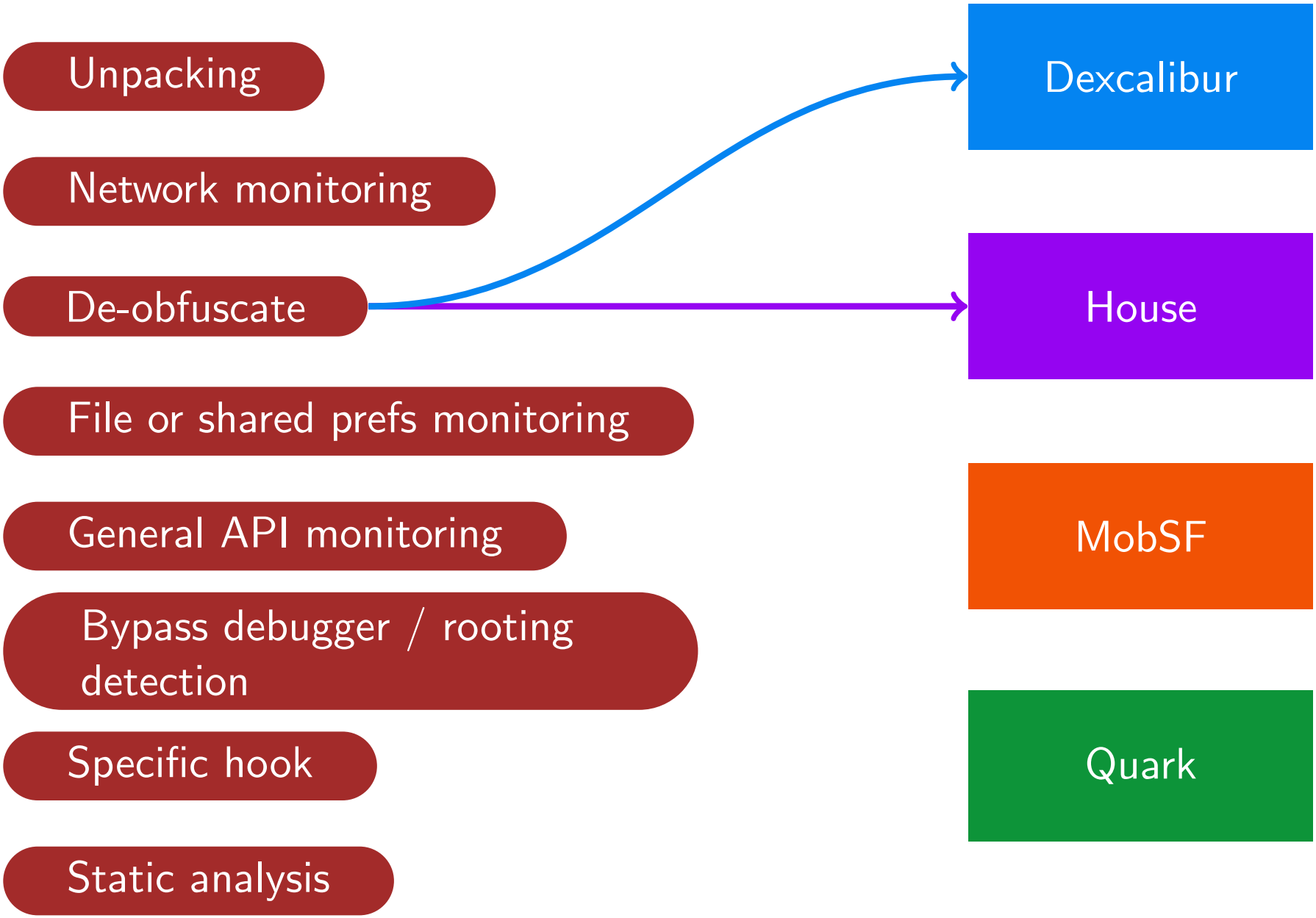
Which tool? (preferred choices only)



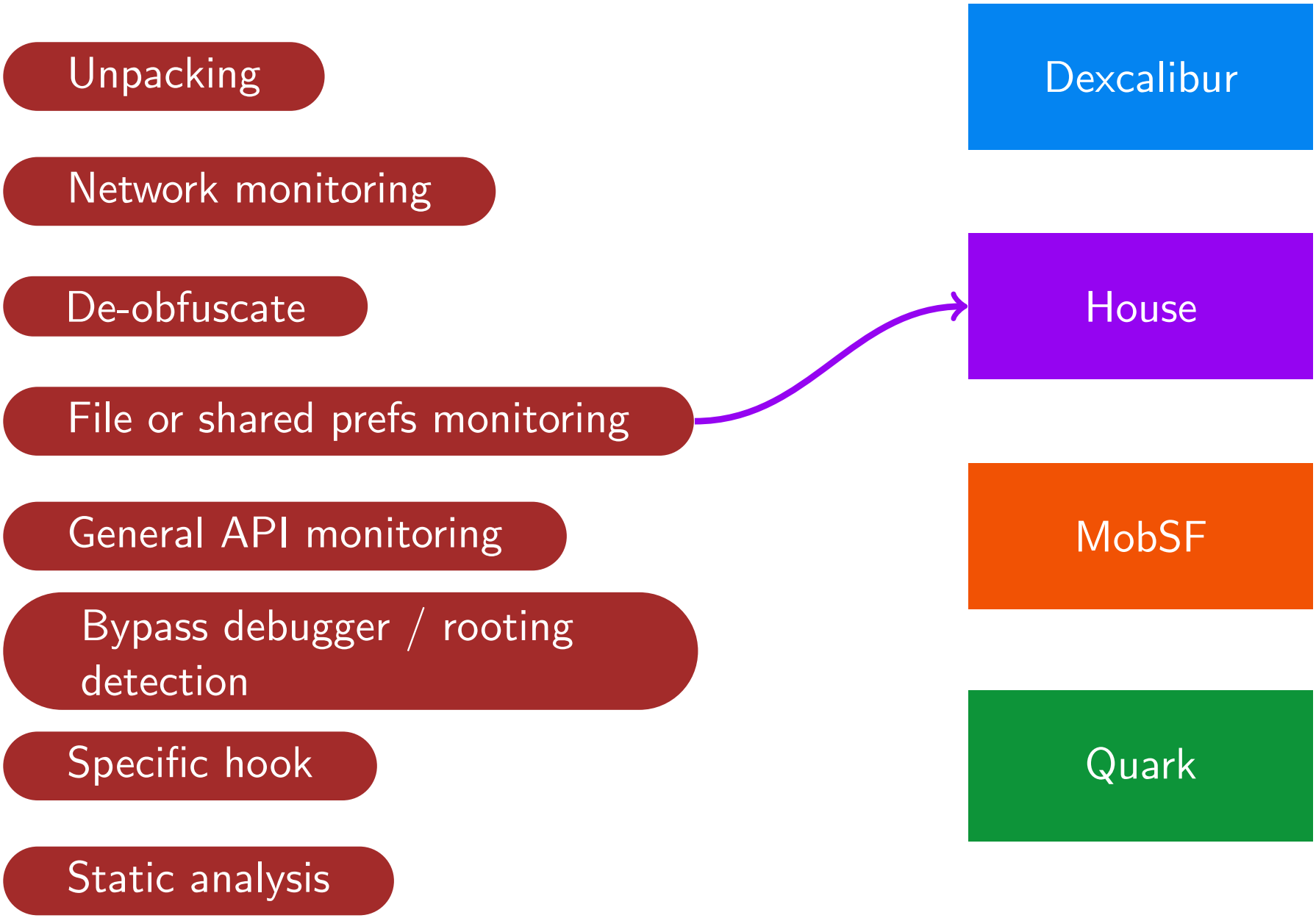
Which tool? (preferred choices only)



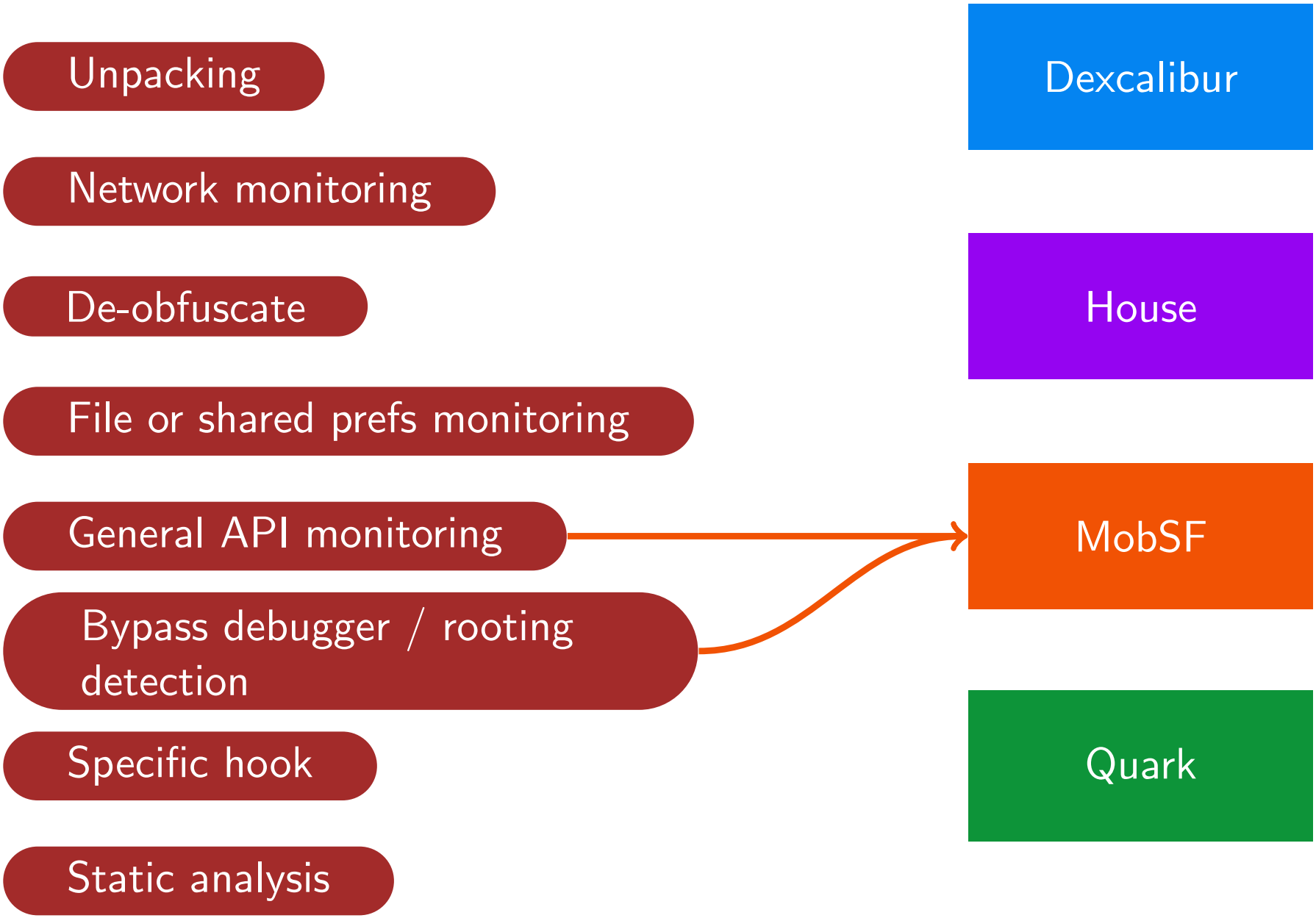
Which tool? (preferred choices only)



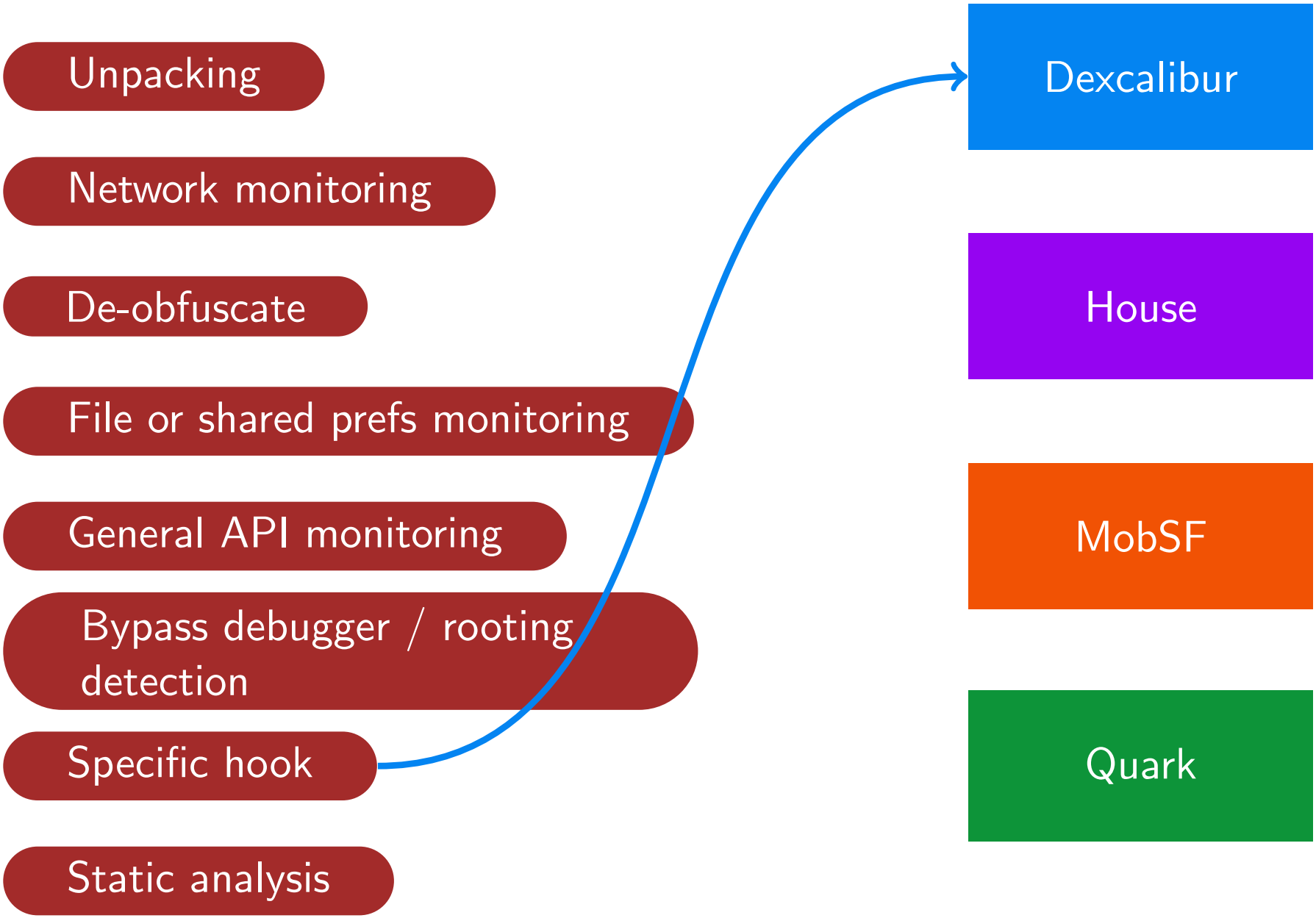
Which tool? (preferred choices only)



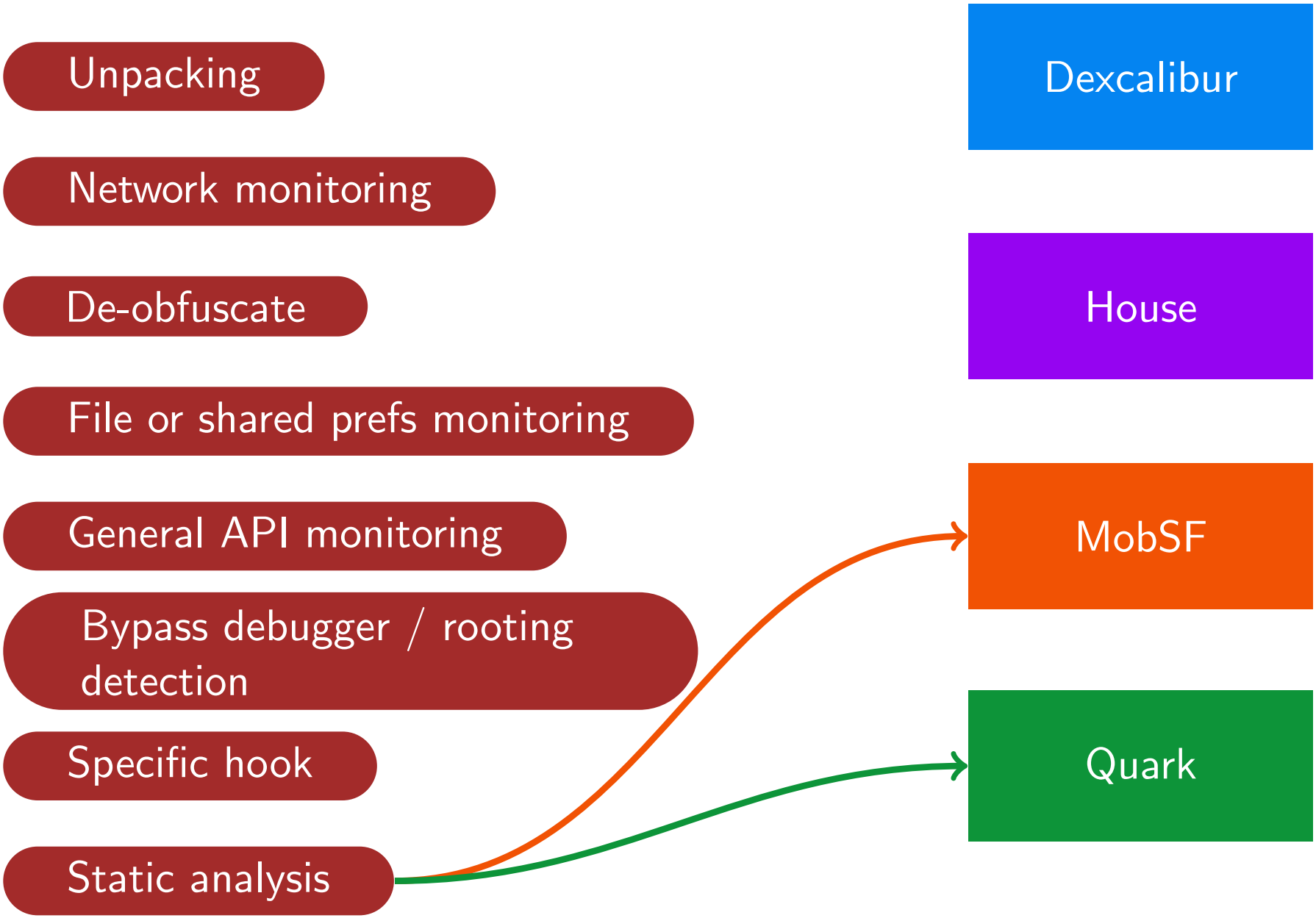
Which tool? (preferred choices only)



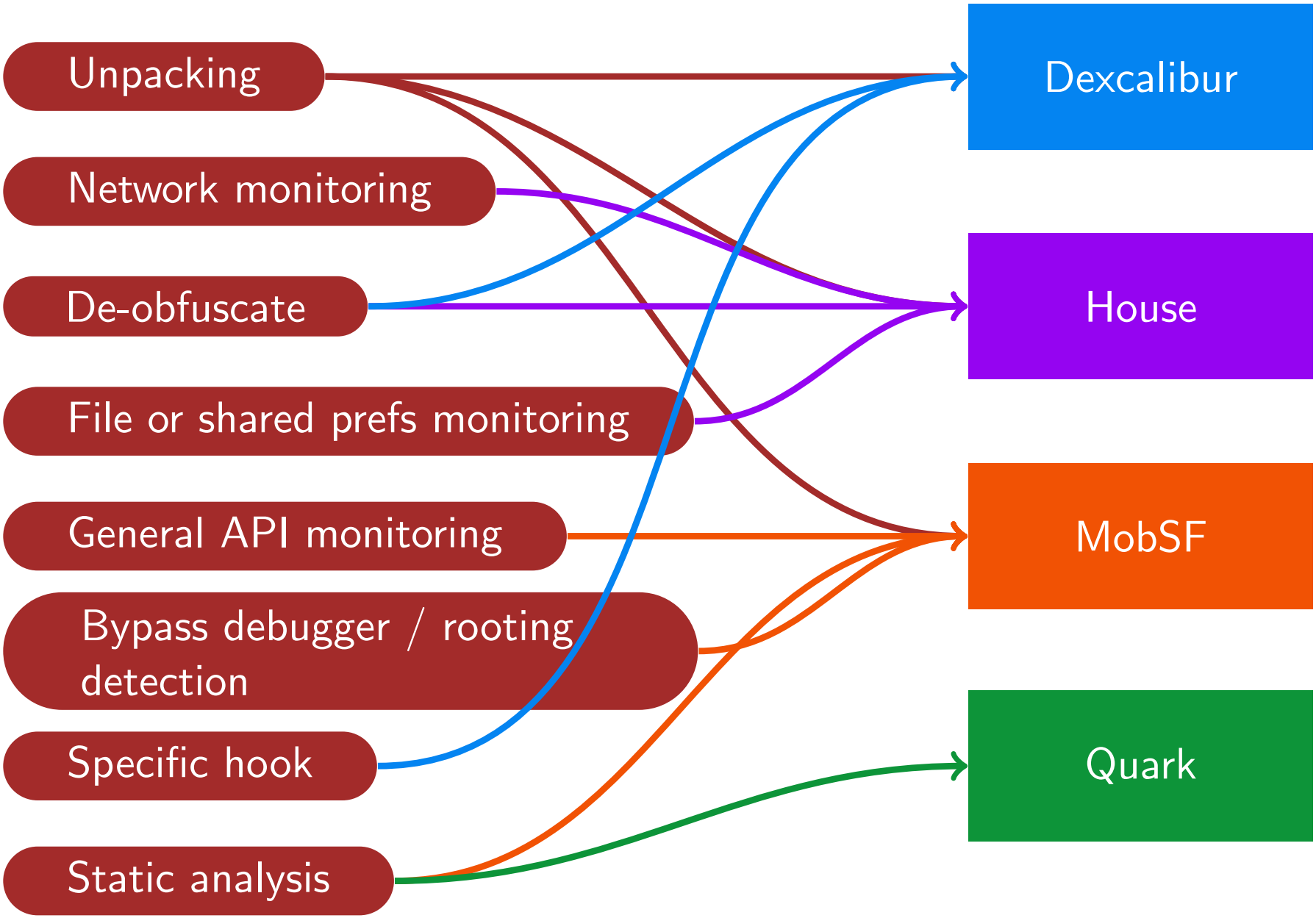
Which tool? (preferred choices only)



Which tool? (preferred choices only)



Which tool? (preferred choices only)



Advanced advanced features?

If you can do it with **Frida**,
you can *probably* do it with [`replace`]
`replace` = `Dexcalibur/House/MobSF`

- In memory DEX loading
- Native unpacking
- Native anti-reversing
- Native de-obfuscation
- ...

but it might be as easy to use Frida *directly*
If you can't do it with Frida.... unlucky!


Thanks for your attention!
Axelle Apvrille
Email: aapvrille (at) fortinet (dot) com
Twitter: @cryptax
FORTINET
AxL
2016