Análisis forense en Android

Introducción

Jorge Coronado

QUANTIKA 14

¿Qué vamos a ver?

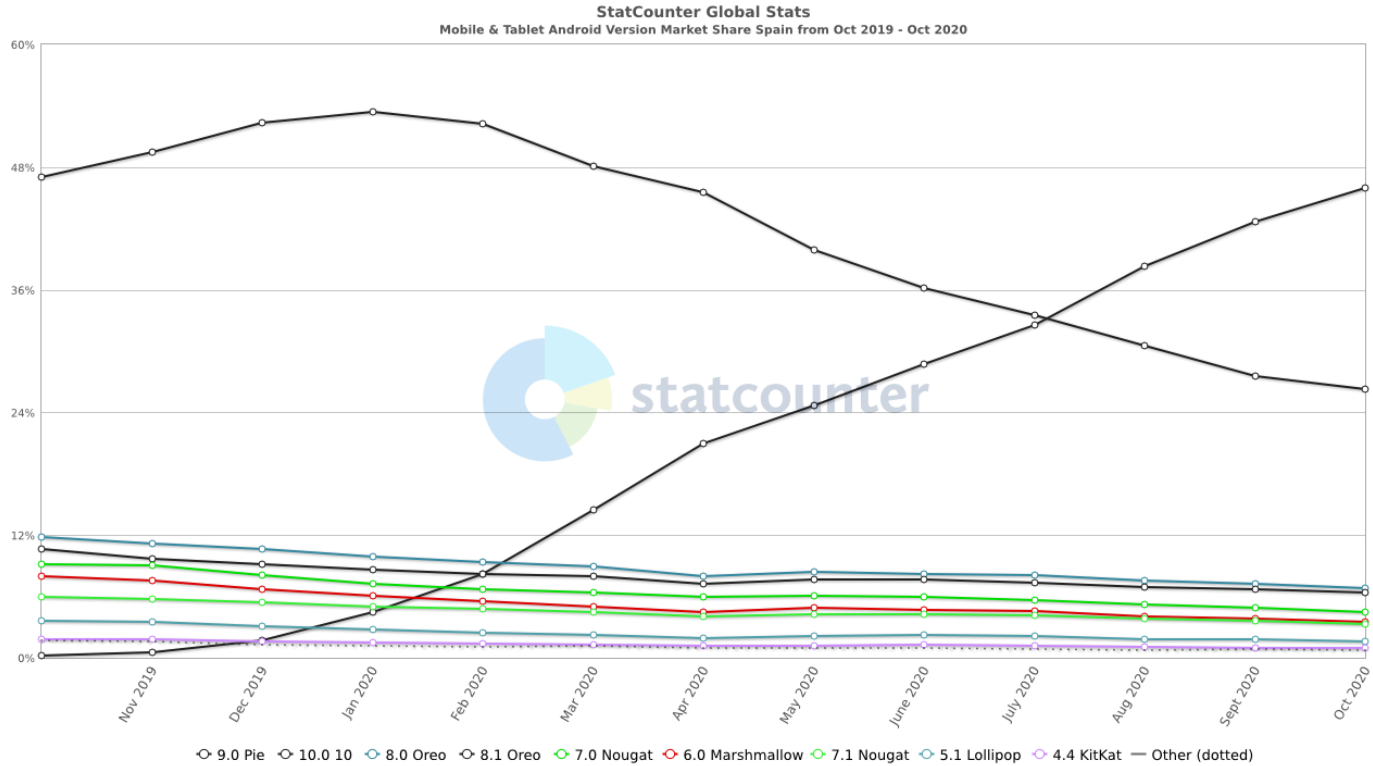
1. El sistema operativo de Android y el forense
2. Experiencia laboral y casos reales
3. Profesionales en España
4. Profesionales fuera de España
5. Aplicaciones más populares

¿Qué vamos a ver en el curso?

1. Metodología
2. Aplicaciones para extracción y clonado
3. Aplicaciones para análisis
4. Peritaje informático en WhatsApp
5. Peritaje informático para identificar ubicación del

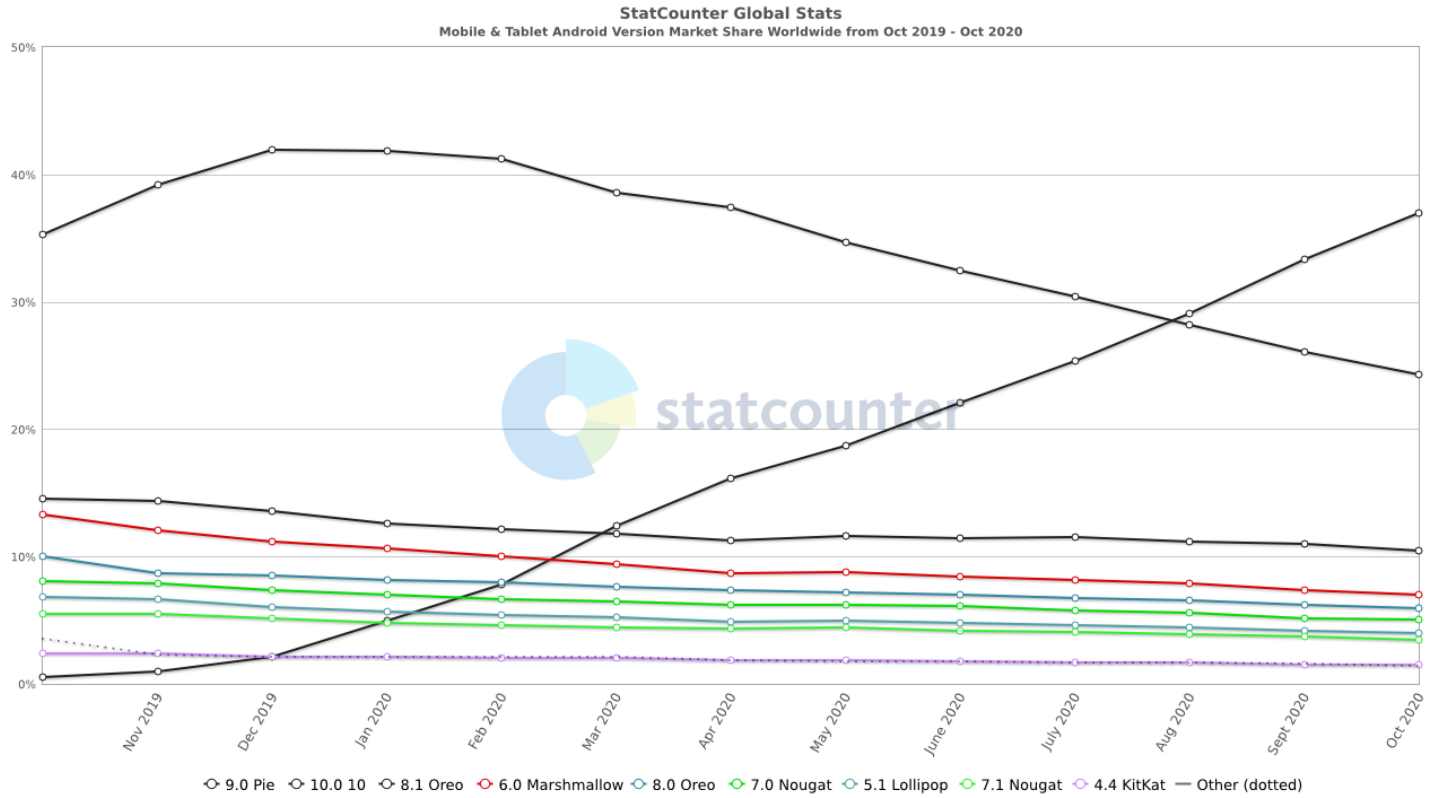
¿QUÉ ES EL ANÁLISIS FORENSE EN ANDROID?

QUANTIKA 14



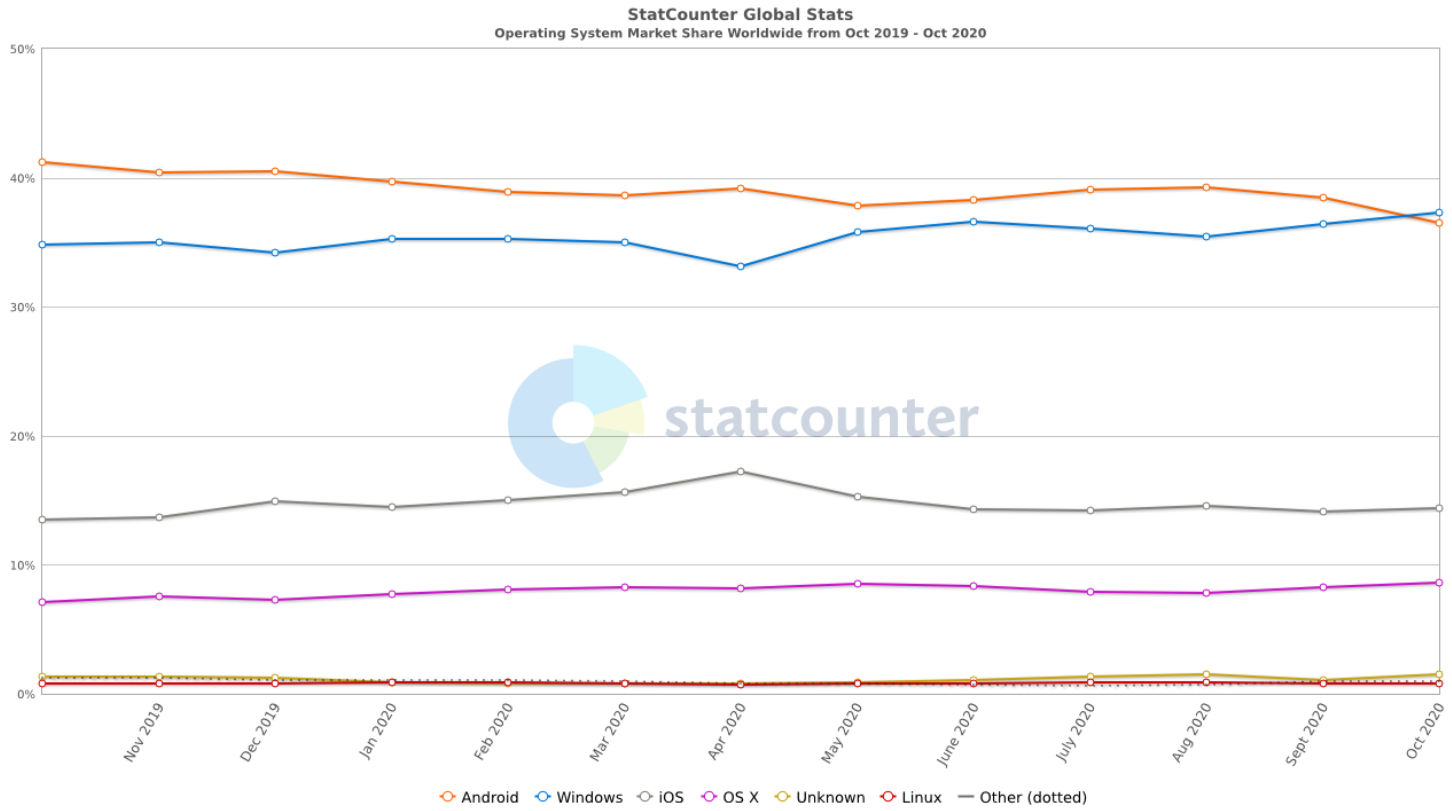
https://gs.statcounter.com/android-version-market-share/mobile-tablet/spain

QUANTIKA 14



https://gs.statcounter.com/android-version-market-share/mobile-tablet/spain

QUANTIKA 14



https://gs.statcounter.com/os-market-share

MI EXPERIENCIA LABORAL

QUANTIKA 14

PROFESIONALES EN ESPAÑA

- Buenaventura Salcedo
  - https://www.youtube.com/watch?v=fhWqLeQDA9o
- Lorenzo Martinez
  - https://www.abc.es/tecnologia/informatica/software/abci-pegasus-software-espia-empresa-israeli-amenaza-democracia-202007151311_noticia.html
- Antonio Sanz (https://twitter.com/antoniosanzalc)
- Jorge Coronado
  - https://blog.quantika14.com/blog/2019/04/05/diario-de-un-perito-informatico-forense-a-un-android-donde-estuvo-nuestro-cliente-sin-ser-root/
  - https://retina.elpais.com/retina/2020/09/25/tendencias/1601043492_414096.html

QUANTIKA 14

PROFESIONALES FUERA DE ESPAÑA

- Andrew Hoog
  - https://www.sciencedirect.com/book/9781597496513/android-forensics#book-info
- Oleg Skulnin
  - https://www.linkedin.com/in/oleg-skulkin-96652a87/
- Denis Sazonov
  - Creador de Andriller https://github.com/den4uk/

APLICACIONES MÁS CONOCIDAS

DE PAGO

- Cellebrite UFED
- Oxygen Forensic
- MobilEdit
- Elcomsoft

GRATUITAS

- Andriller
- Guasap Forensic
- Linux Memory Extractor (LIME) – La extracción de la memoria se debe hacer por la red