Digital Signature Management Course

Every interaction with a digital device creates a signature. These signatures are accessible to third-parties and can reveal sensitive information about your location, activities, and associations. Managing this information properly can help protect your sensitive information, intellectual property and provide a higher level of safety and security. Digital Signature Management (DSM) is a two-day course of instruction focused on building skills to manage and manipulate your digital signature. In DSM you will learn how you and your digital devices interact with the internet, what types of data your devices leak to third-parties, and how you can use countermeasures to protect your sensitive information and activities.

Course Topics Cover:
- Internet and cellular networks
- Building your threat model
- Determining your digital signature
- Information security for complex threat models
- Operational security (OPSEC)
- Manipulating your digital signature
- Non-attributable internet communications and activity
- Operational countermeasures

Course length: 2 days (16 hours)
Prerequisites: Familiar with LINUX, iOS, Android OS's, basic internet tasks such as command line, file creation, downloading, file transfer
Optional modules:
- OPSEC practical 1 day (10 hours)
- Advanced counter-tracking techniques 1 day (10 hours)

All course materials and hardware provided