

# Mobile-based Security Incident Handling Toolkit

Listed below are the tools that help incident handlers in responding to mobile-based security incidents.

Mobile-based Security Incident Handling Tools	
Category	Tools
Mobile Device Monitoring Tools	<ul style="list-style-type: none"><li>▪ Kandji (<a href="https://www.kandji.io">https://www.kandji.io</a>)</li><li>▪ Citrix Endpoint Management (<a href="https://www.citrix.com">https://www.citrix.com</a>)</li><li>▪ Scalefusion MDM (<a href="https://scalefusion.com">https://scalefusion.com</a>)</li><li>▪ IBM MaaS360 (<a href="https://www.ibm.com">https://www.ibm.com</a>)</li><li>▪ VMware AirWatch (<a href="https://www.vmware.com">https://www.vmware.com</a>)</li></ul>
Network Traffic Analysis Tools	<ul style="list-style-type: none"><li>▪ Wireshark (<a href="https://www.wireshark.org">https://www.wireshark.org</a>)</li><li>▪ tcpdump (<a href="https://www.tcpdump.org">https://www.tcpdump.org</a>)</li><li>▪ FaceNiff (<a href="http://faceniff.ponury.net">http://faceniff.ponury.net</a>)</li><li>▪ PCAPdroid (<a href="https://play.google.com">https://play.google.com</a>)</li><li>▪ Network Analyzer Pro (<a href="https://apps.apple.com">https://apps.apple.com</a>)</li></ul>
Android Malware Analysis Tools	<ul style="list-style-type: none"><li>▪ DeGuard (<a href="http://apk-deguard.com">http://apk-deguard.com</a>)</li><li>▪ ClassyShark (<a href="https://github.com">https://github.com</a>)</li><li>▪ Argus-SAF (<a href="http://pag.arguslab.org">http://pag.arguslab.org</a>)</li><li>▪ AppMon (<a href="https://github.com">https://github.com</a>)</li><li>▪ Quark (<a href="https://github.com">https://github.com</a>)</li></ul>
Reverse Engineering Tools	<ul style="list-style-type: none"><li>▪ Frida (<a href="https://frida.re">https://frida.re</a>)</li><li>▪ Radare2 (<a href="https://radare.org">https://radare.org</a>)</li><li>▪ Apktool (<a href="https://ibotpeaches.github.io">https://ibotpeaches.github.io</a>)</li><li>▪ JADX (<a href="https://github.com">https://github.com</a>)</li><li>▪ GDA-android-reversing-Tool (<a href="https://github.com">https://github.com</a>)</li></ul>
Mobile Data Acquisition Tools	<ul style="list-style-type: none"><li>▪ Cellebrite UFED (<a href="https://cellebrite.com">https://cellebrite.com</a>)</li><li>▪ XRY (<a href="https://www.msab.com">https://www.msab.com</a>)</li><li>▪ Oxygen Forensics (<a href="https://www.oxygen-forensic.com">https://www.oxygen-forensic.com</a>)</li><li>▪ Belkasoft Acquisition Tool (<a href="https://belkasoft.com">https://belkasoft.com</a>)</li><li>▪ MOBILedit Forensic (<a href="https://www.mobiledit.com">https://www.mobiledit.com</a>)</li></ul>
Log Analysis Tools	<ul style="list-style-type: none"><li>▪ SolarWinds® Loggly® (<a href="https://www.loggly.com">https://www.loggly.com</a>)</li><li>▪ pCloudy (<a href="https://www.pcloudy.com">https://www.pcloudy.com</a>)</li></ul>

	<ul style="list-style-type: none"> <li>▪ NXLog Enterprise Edition (<a href="https://nxlog.co">https://nxlog.co</a>)</li> <li>▪ LogRabbit (<a href="http://lograbbit.com">http://lograbbit.com</a>)</li> <li>▪ LogViewer (<a href="https://github.com">https://github.com</a>)</li> </ul>
<b>Tools for Investigating Mobile-based Security Incidents</b>	<ul style="list-style-type: none"> <li>▪ Mobile Verification Toolkit (MVT) (<a href="https://docs.mvt.re">https://docs.mvt.re</a>)</li> </ul>
<b>Tools for Analyzing iOS Network Traffic</b>	<ul style="list-style-type: none"> <li>▪ Wireshark (<a href="https://www.wireshark.org">https://www.wireshark.org</a>)</li> <li>▪ Network Analyzer Pro (<a href="https://apps.apple.com">https://apps.apple.com</a>)</li> </ul>
<b>Android-based Log Analysis Tools</b>	<ul style="list-style-type: none"> <li>▪ LogRabbit (<a href="http://lograbbit.com">http://lograbbit.com</a>)</li> <li>▪ Google Admin Toolbox Log Analyzer (<a href="https://toolbox.googleapps.com">https://toolbox.googleapps.com</a>)</li> <li>▪ logentries (<a href="https://logentries.com">https://logentries.com</a>)</li> <li>▪ SolarWinds® Loggly® (<a href="https://www.loggly.com">https://www.loggly.com</a>)</li> <li>▪ LogViewer (<a href="https://github.com">https://github.com</a>)</li> <li>▪ xLog (<a href="https://github.com">https://github.com</a>)</li> </ul>
<b>iOS-based Log Analysis Tools</b>	<ul style="list-style-type: none"> <li>▪ logentries (<a href="https://logentries.com">https://logentries.com</a>)</li> <li>▪ Datadog (<a href="https://www.datadoghq.com">https://www.datadoghq.com</a>)</li> <li>▪ 3uTools (<a href="http://www.3u.com">http://www.3u.com</a>)</li> <li>▪ OkCat (<a href="https://github.com">https://github.com</a>)</li> <li>▪ iDevice Panic Log Analyzer (<a href="https://github.com">https://github.com</a>)</li> <li>▪ JustLog (<a href="https://github.com">https://github.com</a>)</li> </ul>
<b>Android Security Tools</b>	<ul style="list-style-type: none"> <li>▪ ESET Mobile Security Antivirus (<a href="https://www.eset.com">https://www.eset.com</a>)</li> <li>▪ Avast Premium Security (<a href="https://www.avast.com">https://www.avast.com</a>)</li> <li>▪ Bitdefender Mobile Security (<a href="https://www.bitdefender.com">https://www.bitdefender.com</a>)</li> <li>▪ Avira Antivirus Security for Android (<a href="https://www.avira.com">https://www.avira.com</a>)</li> <li>▪ Kaspersky Internet Security for Android (<a href="https://www.kaspersky.com">https://www.kaspersky.com</a>)</li> <li>▪ Trend Micro™ Mobile Security for Android™ (<a href="https://www.trendmicro.com">https://www.trendmicro.com</a>)</li> </ul>
<b>iOS Security Tools</b>	<ul style="list-style-type: none"> <li>▪ Avira Mobile Security (<a href="https://www.avira.com">https://www.avira.com</a>)</li> <li>▪ McAfee® Total Protection (<a href="https://www.mcafee.com">https://www.mcafee.com</a>)</li> <li>▪ Kaspersky Total Security (<a href="https://www.kaspersky.com">https://www.kaspersky.com</a>)</li> <li>▪ Trend Micro™ Mobile Security for iOS (<a href="https://www.trendmicro.com">https://www.trendmicro.com</a>)</li> <li>▪ Norton360 Antivirus &amp; Security (<a href="https://us.norton.com">https://us.norton.com</a>)</li> <li>▪ LogDog (<a href="https://getlogdog.com">https://getlogdog.com</a>)</li> </ul>