ACCCF / 应用知识图书馆

13

卷

在删除或指控之前作出安全决定

西班牙语版 · 2026

怀疑遭受数字监控：Zero Breach Toolkit 核查与证据保存指南

危机、虚假线索、经验证的下载、隐私、报告解读与鉴定交付

帮助担忧的人核查线索，同时不破坏证据、不引入其他风险，提供简单步骤，并为案件复核人员附上可复现的附录。

面向担心手机或电脑安全的任何人，以及受理此类案件的鉴定人。无需掌握入侵、物理提取、JTAG 或 chip-off 知识。本地核查是可选项；寻求帮助绝不以完成本地核查为前提。

编辑统筹：Jocsan Laguna · 美洲网络安全与计算机取证委员会

通用技术指南与开放教育材料。不构成法律意见、专家鉴定意见，也不提供未经授权访问系统的指导。示例和数据均为虚构；图示为编辑重构。

目录

所示页码对应 PDF 版。Word 可在打开文档时更新本目录；标题保留内部导航。

1. 在触碰任何内容之前：保持安全与冷静 3
2. 可能看似间谍活动的正常行为 4
   2.1 信号不等于解释 4
   2.2 误报不等于凭空想象 4
3. Zero Breach 的用途及不应使用的情形 5
   3.1 对公开线索进行本地核查 5
   3.2 何时停止并寻求帮助 6
4. 软件包下载与验证 6
   4.1 官方仓库，不使用转发链接 6
   4.2 Windows 可执行文件验证 7
   4.3 替代方案：源代码与可复现比较 7
5. 运行前的隐私与准备 7
   5.1 本地运行不等于无害 7
   5.2 文件夹与范围准备 8
   5.3 预览与描述 8
6. 分步执行 9
   6.1 第一步：先练习，不检查真实设备 9
   6.2 随后：经授权的本地检查 9
   6.3 如果选择检查手机 10
7. 分享前如何解读报告 10
   7.1 结果、等级、范围与缺口 10
   7.2 代码及操作含义 10
   7.3 “Worth a look”不是定论 11
8. 实验室的四个场景 12
   8.1 `spyware`：六项发现，不轻率下结论 12
   8.2 `worth-a-look`：用于提问而非指控的要素 12
   8.3 `clean`：无匹配项，但有四个缺口 12
   8.4 `cellebrite`：取证访问，而非间谍软件 13
9. 安全交付给鉴定人或响应团队 17
   9.1 先交摘要，再交完整案卷 17
   9.2 用于可验证交付的 Hash 与 EML 18
   9.3 避免引发第二次危机的说明 18
附录A 鉴定人可复现协议 19
   A.1 环境与来源记录 19
   A.2 经授权实际执行的记录表 19
   A.3 解释矩阵 20
附录B 法律框架、隐私与最终检查 20

1. 在触碰任何内容之前：保持安全与冷静

如果你认为有人在监视你的手机或电脑，首先要做的不是下载程序，而是避免因仓促而丢失信息或引发其他问题。不要删除文件、不要重置设备、不要安装号称万能的工具套件，也不要允许陌生人通过远程访问控制设备。担忧可能源于正常功能、某项配置或真实事件。目前我们尚不清楚原因，也无需在这一分钟就作出判断。

如存在人身威胁、未成年人面临风险、正在遭受跟踪追逐，或有人可能发现你正在求助，应优先保障人身安全并使用当地紧急渠道。不要仅因为本指南提供了方法就运行核查。分析可能更改记录、占用空间，或间接提醒控制该环境的人。继续操作前，应通过安全设备和安全渠道寻求帮助。

列一份简短清单：观察到了什么、何时开始、发生了什么变化、安装了什么、谁曾物理接触设备，以及哪些账户可能遭入侵。记不得准确时间时，使用约略时间。不要为了求助而截取或转发私密内容。一条消息、一个 URL、一项设置、一个应用名称和一个日期，通常比装满你整个私生活的文件夹更有用。

> **必要信息优先于可能信息**
>
> 深呼吸。不要删除，不要追逐所谓的攻击者，也不要分享密码或验证码。如有危险，立即求助。如有时间，只保存必要材料，冷静核查。Duriva 会多次问你：你能证明什么，什么又只是看似可能？



图1. 核查之前，避免丢失来源。首要任务不是证明自己判断正确。编辑重构；不构成真实证据。

2. 可能看似间谍活动的正常行为

2.1 信号不等于解释

不同的 MAC 地址、一次断连、电池电量快速下降、意外通知、陌生应用或新的 IP 地址，各自本身都不能证明有人在监视你。它们可能源于隐私功能、更新、信号覆盖、同步、合法应用或共享账户，也可能是更严重问题的一部分。错误在于尚未检查来源，就选择最令人警觉的解释。

Apple 文档说明，其设备可以针对不同网络使用不同的私有 Wi-Fi 地址；在兼容系统上启用 Rotating 模式时，还可以每两周更换一次。该功能旨在减少跟踪，并不能证明间谍活动。断连则是另一个问题：可能涉及路由器、覆盖、更新、兼容性、电源、软件或企业配置。未经检查，不要将其归因于单一原因。[1]

观察到的现象	首先冷静核查	保存什么以供复核
MAC 地址发生变化	检查各网络的私有地址设置以及设备型号 / 系统。	保存设置、网络和日期截图；不要保存整个历史记录。
设备断连	记录频率、其他设备、覆盖情况、时间和近期变更。	型号、系统、路由器、模式和错误；不要保存 Wi-Fi 密码。
电池电量下降很快	检查各应用的耗电、信号、温度和更新情况。	系统统计数据和时段，不要保存聊天内容。
消息重复	检查同步、其他设备和已关联账户。	应用、版本、时间、账户和相关上下文消息。
安全警报	查看工具检测到哪个文件或行为，以及工具的版本。	完整警报、路径、日期和说明；不要运行该文件。
夜间活动	区分更新、备份、任务和物理访问。	记录、锁定状态和谁曾持有设备。

2.2 误报不等于凭空想象

误报是指警报并不代表所担忧的问题，但并非所有异常行为都是误报，也并非所有未发现异常的结果都是误报。当事人不需要别人说自己是在胡思乱想，而需要知道哪项核查会改变解释。如果某项配置能够解释相关数据，应记录在案；如果不能解释，就继续调查，既不责备，也不轻率下结论。

[1] Apple Support。《Use private Wi-Fi addresses on Apple devices》：私有地址可能因网络而异，在兼容系统中启用 Rotating 时每两周变化一次。该功能旨在减少跟踪；既不构成间谍活动证据，也不能解释所有断连。 官方在线来源

正确的说法

“这可能有正常解释。我会先核实，再决定是否称其为间谍活动。”同时也应说：“如果这个解释说不通，我会保存来源，交由具备资质的人员复核。”



图2. 信号不等于解释。先核查，再解释。编辑重构；不构成真实证据。

3. Zero Breach 的用途及不应使用的情形

3.1 对公开线索进行本地核查

Zero Breach Toolkit 是一款免费开源工具，可在计算机、Android 采集数据和 iPhone 备份中查找某些间谍软件的公开记录指标。它可以检查文件、浏览器、持久化记录和其他受支持的取证工件。它不是完整的取证鉴定，不能发现所有监控，也不能因为没有发现异常就证明一个人是安全的。[2][3]

当你希望在本地初步查看已知线索，并获得明确列出的未检查项目时，这款工具尤其有用。它的价值不在于宣称“没有鬼怪”，而在于区分巧合、薄弱参考、缺口和需要专家回答的问题。新的或未知来源不会自动出现在公开指标库中，一些痕迹还会随时间消失。

[2]Zero Breach Toolkit，仓库 interplains/Zero-Breach-Toolkit。对公开的间谍软件指标进行本地核查，代码采用 Apache 2.0 许可，并附有范围与限制文档。 官方在线来源

[3]Zero Breach Toolkit。按核查类别划分的覆盖范围与限制：文件、浏览器、持久化、记录、Android 和 iPhone 备份。不衡量检测率或误报率。 官方在线来源

3.2 何时停止并寻求帮助

如果核查可能使你陷入危险、你未获授权使用设备或文件、他人可能观察核查过程，或你无法保护报告，就不要运行核查。也不要在未经许可的情况下，用它检查伴侣、员工、客户或亲属的设备。能够读取某个文件，并不意味着你是获得授权的内容所有者。

如果已经有可信的安全通知、已确认的数据提取或定向攻击疑虑，应寻求专业帮助，无需先完成自己的检查。记者、活动人士、人权捍卫者和民间社会人员可以联系 Access Now 帮助热线或 Amnesty International Security Lab，相关链接见报告本身。其他任何人则应联系事件响应人员或具备资质的鉴定人。[4]

情形	首先怎么做	应避免的做法
对异常行为感到好奇	扫描前检查设置和时间线。	随意安装大量工具。
合理怀疑且环境安全	在明确范围和隐私要求后进行本地核查。	在群组中分享完整报告。
危险或正在进行的监视	寻求专业帮助，使用安全设备 / 渠道。	运行可能暴露求助行为的测试。
他人的设备	明确授权并记录范围。	仅因能够访问就阅读内容。
指南或课程练习	使用内置合成场景，不使用真实设备。	将训练结果当作真实检测。

> **你无需成为黑客**
>
> 无需进行 test point、通过处理器访问或实施 chip-off。如果简单核查无法回答问题，应保存现有材料并交由专业人员处理。技术复杂性不是寻求帮助的前提。

4. 软件包下载与验证

4.1 官方仓库，不使用转发链接

本指南使用的来源是 `github.com/interplains/Zero-Breach-Toolkit`。从该处打开 Releases 部分，下载适用于 Windows、macOS 或 Linux 的软件包或源代码。不要从视频、短链接、截图或评论中下载同名文件。名称相同并不能证明内容相同。[5]

[4] Zero Breach Toolkit。合成训练场景指南：spyware、worth-a-look、clean 和 cellebrite。指标均为虚构，示例不读取设备或真实列表；不能据此推断真实设备的状态。 官方在线来源

[5] Zero Breach Toolkit，仓库 interplains/Zero-Breach-Toolkit。对公开的间谍软件指标进行本地核查，代码采用 Apache 2.0 许可，并附有范围与限制文档。 官方在线来源

项目文档说明，Windows 程序未使用代码签名证书签名，因此 SmartScreen 或防病毒软件可能发出警告。不要关闭保护措施，也不要盲目信任该文件。项目提供构建流程证明；对于较新的程序，还提供签名的 SHA-256 清单。运行前应先验证。[6]

4.2 Windows 可执行文件验证

安装 GitHub CLI 并将可执行文件下载到当前文件夹后，文档建议进行以下来源验证：

验证的是构建证明，而不是不存在恶意软件

```
gh attestation verify zero-breach-toolkit-windows-x64.exe --repo interplains/Zero-Breach-Toolkit
```

有效的构建证明将这些字节与公开构建流程及一个 commit 关联起来，但不能证明程序没有错误，也不能证明它适合你的情况。你还可以使用项目所述的签名 SHA-256 清单。不要把在其他页面找到的 hash 当作自己文件的 hash：应自行计算，并与该版本对应的官方来源进行比较。

4.3 替代方案：源代码与可复现比较

另一种途径是克隆仓库、审查代码，并将生成的 Python 文件与预期版本比较。项目介绍了单文件的确定性构建和发布验证。非技术人员不必自行编译：可以请人帮助验证软件包，或使用菜单中的练习选项。不应为了赶时间而跳过来源身份核实。

官方代码获取示例

```
git clone --depth 1 https://github.com/interplains/Zero-Breach-Toolkit.git
```

> **Duriva 提问**
>
> 这个可执行文件究竟来自哪里？如果无法说明仓库、版本和验证方式，就还不到运行它的时候。

5. 运行前的隐私与准备

5.1 本地运行不等于无害

常规分析在设计上不会上传你的数据，也不会访问指标。更新列表确实会使用网络；Android 采集则会在征得同意后下载独立的收集器，并改变手机状态。此外，内部网络阻断并不是操作系统沙箱：网络挂载、其他应用和同步仍然存在。如需严格隔离，应与专家共同决定。[7]

[6] Zero Breach Toolkit。版本验证指南：GitHub Actions 构建程序的证明、SHA-256 清单和签名；Windows 软件包没有 Windows 代码签名。 官方在线来源

[7] Zero Breach Toolkit。PRIVACY：常规分析在设计上不执行上传；更新与 Android 采集是不同活动。报告可能包含敏感数据，分享摘要不能替代完整报告。 官方在线来源

报告可能包含用户名、个人资料、路径、历史记录、SMS 发件人和消息摘录。分享摘要包含的信息较少，但不是完整的取证鉴定，未经审查也不应公开。选择未同步的本地文件夹，避免使用 OneDrive、iCloud、Dropbox 和共享文件夹，并决定谁可以打开报告。不要向仓库发送密钥、cookie、密码或个人文件。

5.2 文件夹与范围准备

决定事项	如何选择	原因
输出文件夹	本地新建、不同步且限制访问。	避免泄露历史记录和路径。
首次运行	练习场景或限定范围。	了解报告，而不虚构真实案例。
指标更新	独立且知情的步骤，不要与扫描混淆。	网络和数据源会变化。
已打开的应用	按程序要求关闭浏览器和消息应用。	减少文件锁定和并发更改。
权限	仅限必要权限；不要习惯性地提升权限。	避免检查其他账户或更改配置。
接收结果的人	创建文件前确定接收人和安全渠道。	避免事后一时冲动进行分享。

5.3 预览与描述

分析真实数据之前，可以先查看范围和可用的核查项目。`--preview` 展示范围而不扫描；`--describe` 以 JSON 返回有哪些读取项及其限制。这些步骤有助于判断核查能否回答问题，以及是否存在侵入性更低的替代方案。[8]

范围与读取项说明

```
python -X utf8 scan/zero-breach-toolkit.py --preview
python -X utf8 scan/zero-breach-toolkit.py --describe
```

> **继续操作之前**
>
> 如果范围包含你无需分享的数据，应缩小选择范围。如果当前担忧需要专业帮助，不要为了完成这些步骤而推迟求助。工具是一种选择，不是义务。

[8]Zero Breach Toolkit。结果与覆盖约定：代码0、1、2、3和4；区分发现、参考、缺口、未扫描退出和有限范围。无匹配结果绝不是安全保证。 官方在线来源

6. 分步执行

6.1 第一步：先练习，不检查真实设备

项目包含为学习而创建的场景：`spyware`、`worth-a-look`、`clean` 和 `cellebrite`。它们使用虚构的手机和指标，以及不可能属于真实基础设施的 `.invalid` 域名。报告带有醒目的训练警告，临时目录会在结束后删除。这些场景不会生成分享摘要或证据包，因为不应有人将其误认为真实案例。[9]

四个练习场景

```
python scan/zero-breach-toolkit.py --training spyware
python scan/zero-breach-toolkit.py --training worth-a-look
python scan/zero-breach-toolkit.py --training clean
python scan/zero-breach-toolkit.py --training cellebrite
```

如果使用 Windows 启动器，请在菜单中寻找练习选项；文档将其标为 `Practise`。如果使用源代码，请从仓库文件夹运行命令。不要将 `--training` 与真实文件、手机、更新或列表结合使用：程序在设计上会拒绝这种组合。先了解结果、证据等级和缺口分别显示在哪里。

6.2 随后：经授权的本地检查

当来源已经验证、授权明确且输出文件夹受到保护后，可以运行所选范围的检查。如果想避免刻意造成覆盖不完整，就不要使用 `--quick`。如果选择特定目标，应明确知道自己选择了什么：针对性检查不等于检查整台设备。

生成报告、JSON 和最简摘要的执行示例

```
python -X utf8 scan/zero-breach-toolkit.py --report reporte.txt --json reporte.json --share-json
resumen.json
```

文本报告供阅读，JSON 供检查结构，摘要供以较少信息暴露开展首次沟通。三者均不能证明设备的真实性，也不能证明整个系统都已检查。不要将训练与 `--share-json` 或证据包结合使用：后两者仅为经授权的真实检查生成。

[9] Zero Breach Toolkit。合成训练场景指南：spyware、worth-a-look、clean 和 cellebrite。指标均为虚构，示例不读取设备或真实列表；不能据此推断真实设备的状态。 官方在线来源

6.3 如果选择检查手机

Android 采集与 iPhone 备份检查并不相同。工具读取可用的取证工件，并说明无法访问的内容。采集会改变手机状态并保存私人信息；未经明确同意、没有安全存储位置且不了解覆盖范围，就不要进行采集。本地副本可能需要单独的密码或解密；不要分享，也不要上传到分析服务。[10][11]

> **没有“真相按钮”**
> 如果不知道刚刚选择了什么范围，请停止操作。答案不在于点击“full”，而在于弄清哪些内容已经检查、哪些内容无法检查。

7. 分享前如何解读报告

7.1 结果、等级、范围与缺口

在看任何数字之前，先读四项内容：结果作出了什么论断、证据等级如何、检查了什么范围，以及哪些内容未纳入。同一个数字可能因来源不同而具有不同含义。六项发现不等于六起感染，零项发现不等于没有监控，一条引用也不等于正在运行的恶意文件。

要素	提供的信息	可避免的错误
结果与代码	所选执行中发生了什么。	将其变成绝对标签。
证据等级	属于文件、记录、引用、日志还是基础设施。	将一切视为执行证据。
范围	包括哪些手机、文件、账户和选项。	推广到整台设备。
缺口	哪些内容无法读取或核查，以及原因。	将未检查内容称为“干净”。
指标与日期	使用了哪些来源，以及是否为最新。	将最近的副本误认为当前指标。
下一步	根据情况保存证据、补齐缺口或寻求帮助。	本能地删除或“清理”。

7.2 代码及操作含义

代码 / 情形	正确解读	下一步决定
0：没有可处置项或缺口	该范围内未发现可处置的匹配项。	不要据此称设备安全；复核范围和担忧原因。

[10] Zero Breach Toolkit。按核查类别划分的覆盖范围与限制：文件、浏览器、持久化、记录、Android 和 iPhone 备份。不衡量检测率或误报率。 官方在线来源

[11] Zero Breach Toolkit。PRIVACY：常规分析在设计上不执行上传；更新与 Android 采集是不同活动。报告可能包含敏感数据，分享摘要不能替代完整报告。 官方在线来源

代码 / 情形	正确解读	下一步决定
1：错误	执行或输出失败。	修正输入或输出位置；不要解释为未发现异常。
2：有可处置匹配项	存在需要解释和保存的线索。	不要删除、运行或追踪；寻求帮助。
3：缺少数据或来源	存在缺口；不是干净结果。	补齐覆盖范围并重新检查。
4：未扫描即退出	未进行核查，也未得出结论。	不要断言不存在间谍软件。
已移除的参考或指标	指标来源的变化会改变其当前含义。	复核背景和来源，不要强行指控。

表格来源：[12]

7.3 “Worth a look”不是定论

从应用商店之外安装的应用、无障碍访问权限、旧版本或已关闭的验证设置，都可能值得询问。仅凭其中任何一项，都不能认定发现了问题。无障碍工具、屏幕阅读器、密码管理器和自动化应用都可能是合法的。了解设备的人可以结合更多信息确认或排除这些解释。

> **Duriva 打破第四面墙**
>
> 如果只读“有六项匹配”，它就像一份判决。如果还读到“有四项核查未执行”，就会明白案卷仍未关闭。这就是立即反应与认真复核的区别。



图3. 报告应分层解读。范围和缺口会改变其含义。编辑重构；不构成真实证据。

[12]Zero Breach Toolkit。结果与覆盖约定：代码0、1、2、3和4；区分发现、参考、缺口、未扫描退出和有限范围。无匹配结果绝不是安全保证。 官方在线来源

8. 实验室的四个场景

8.1 `spyware`：六项发现，不轻率下结论

合成场景 `spyware` 产生了六项匹配：五项设备端证据和一项注册表证据，包括一个应用、一个文件指纹、一个证书、一个属性、一条路径和一个虚构基础设施参考。同时留下四个缺口：无文件指纹、无电池历史记录、无故障报告和无 SMS 备份。结果为 `INDICATORS_FOUND`，代码2，`scan_state: partial`。[13]

这个场景要教的不是“你感染了间谍软件”，而是如何归组不同对象，以及为什么每个对象都需要解释。输出本身也提醒：匹配意味着需要调查，而不是宣布设备失陷或执行清理。文件或配置的存在本身不能证明已经执行，基础设施参考也不能证明成功建立连接。整台手机和所有指标均为虚构。

8.2 `worth-a-look`：用于提问而非指控的要素

`worth-a-look` 场景未发现已知指标，但显示了四个值得询问的要素：一个直接安装且具有无障碍访问权限的应用、过旧的更新、已启用的无障碍服务，以及已关闭的应用验证。结果为 `NO_KNOWN_INDICATORS_WITH_GAPS`，代码3，并有相同的四个覆盖缺口。[14]

这些要素既不能证明感染，也不能证明虚假。它们是在邀请你询问：你认得这个应用吗？为什么安装它？你预期它会获得这项权限吗？是否有待安装的更新？异常行为发生前有什么变化？本手册既不断言设备所有者判断错误，也不断言一切正常。目标是学会先提问，再指控。

8.3 `clean`：无匹配项，但有四个缺口

`clean` 场景未产生已知匹配项，但保留了四个缺口，代码为3。输出明确说明，这不是健康证明。它告诉我们，“未发现任何内容”只能指已检查的范围和已知指标，不能证明不存在新型、隐藏、定向或未见记录的间谍软件，也不能证明所有位置都已检查。[15]

如果一个人有具体理由担忧，这个结果并不会消除担忧。下一步可以是补齐覆盖范围、检查记录、咨询专家，或只是记录首次核查未提供可处置的线索。无需为了让当事人感到被理解而强行得出误报结论。

[13]ACCCF 本地实验室。Zero Breach Toolkit 2.0.6，commit 10ceaba497e40da1f327916a0a3fe0af0ff5994f，运行四个合成场景。spyware、worth-a-look、clean 和 cellebrite 文件，格式为 TXT/JSON。未检查个人信息或真实设备。

[14]ACCCF 本地实验室。Zero Breach Toolkit 2.0.6，commit 10ceaba497e40da1f327916a0a3fe0af0ff5994f，运行四个合成场景。spyware、worth-a-look、clean 和 cellebrite 文件，格式为 TXT/JSON。未检查个人信息或真实设备。

[15]ACCCF 本地实验室。Zero Breach Toolkit 2.0.6，commit 10ceaba497e40da1f327916a0a3fe0af0ff5994f，运行四个合成场景。spyware、worth-a-look、clean 和 cellebrite 文件，格式为 TXT/JSON。未检查个人信息或真实设备。

8.4 `cellebrite`：取证访问，而非间谍软件

`cellebrite` 场景在 USB 注册表中产生了一项匹配，代码为2。其目的是展示工具如何识别取证访问痕迹，以及建议如何随之变化：保存证据、检查该时间点前后的应用；如果背景情况支持，则从另一台设备更改密码。注册表和序列号均为虚构，背后没有任何真实个人或设备。[16]

这个案例不是间谍软件，也不能仅凭它断言已经完成了一次完整提取。取证问题是：谁接触过手机、持续多久、基于什么授权，以及此前和此后发生了什么。结论必须区分连接痕迹与背景能够证实的含义。

> **四点不同启示**
>
> 匹配不等于感染；待检查要素不等于误报；零匹配不等于安全；取证痕迹也不等于完整提取的证据。报告是复核的起点，不是定论。

[16]ACCCF 本地实验室。Zero Breach Toolkit 2.0.6，commit 10ceaba497e40da1f327916a0a3fe0af0ff5994f，运行四个合成场景。spyware、worth-a-look、clean 和 cellebrite 文件，格式为 TXT/JSON。未检查个人信息或真实设备。

ESCENARIO SINTÉTICO · ZERO BREACH TOOLKIT 2.0.6 · spyware

```
########################################################################
  TRAINING EXAMPLE - NOT A REAL CHECK
  Scenario: spyware. This is a made-up phone checked against made-up
  indicators. It says nothing about this computer or any real device.
########################################################################
========================================================================
  Zero Breach Toolkit 2.0.6 - spyware indicator check
  Scope: default (phone evidence only)
  Checks for TRACES of known mercenary spyware. A clean result is NOT a
  clean bill of health - see what could not be checked, below.
  2026-11-10T18:37:33   Windows 11
========================================================================

========================================================================
  SUMMARY  —  read this part
  TRAINING EXAMPLE: a made-up phone and made-up indicators, not a real check.
========================================================================
  RESULT: SERIOUS FINDING - seek expert help promptly.

  WHAT WAS FOUND
    >> SOMETHING THE RESEARCHERS TIE TO SPYWARE IS ON THIS PHONE
       org.example.training.spyapp  [artifact]
          Where: app org.example.training.spyapp

    >> SOMETHING THE RESEARCHERS TIE TO SPYWARE IS ON THIS PHONE
       e36c3fee5d43ffb61b91fbee792cd8b7b4ebd9076f77e9002a9eaa0ea5648a84  [sample]
          The file fingerprint of a published spyware sample (its family
          is named where the source gives one). A match here is
          conclusive, not circumstantial.
          Where: app org.example.training.spyapp (/data/app/training-spyapp/base.apk)

    >> SOMETHING THE RESEARCHERS TIE TO SPYWARE IS ON THIS PHONE
       d472b7c9d957a9e55ce56bd80388b97be9e2132644c0a51cac03aa618905e6d2  [artifact]
          Where: app org.example.training.spyapp

    >> SOMETHING THE RESEARCHERS TIE TO SPYWARE IS ON THIS PHONE
       persist.training.spy.flag  [artifact]
          Where: system property persist.training.spy.flag

    >> SOMETHING THE RESEARCHERS TIE TO SPYWARE IS ON THIS PHONE
       /data/local/tmp/training-spy-daemon  [artifact]
          Where: /data/local/tmp/training-spy-daemon

    >> THE PHONE'S SYSTEM LOGS NAME THIS SPYWARE INFRASTRUCTURE
       training-spyware-server[.]invalid  [infrastructure]
          A server the cited researchers attribute to the named spyware
          family. Its exact role - delivering an exploit, controlling an
          implant or receiving stolen data - is not stated in the source,
          so treat contact as serious but unspecified. A domain can change
          hands after a campaign ends: compare the date of the evidence
          with the date of the research.
          the phone's own system logs name it - it may have been a
          connection, a lookup, or only text an app wrote to the log
          Where: phone log dumpsys.txt, line 1

  WHAT TO DO
    Seek expert help promptly. Preserve this report and the named
    files or registrations. Do NOT delete, move, run or try to clean
    them. A file match establishes presence; a registration
    establishes configuration. Neither alone establishes that spyware
    executed.

    Contact a qualified incident responder or your organisation's
    security team. You do not need to finish investigating first.
    Support options are at the end of this report.
```

Fragmento literal del reporte real de entrenamiento. No representa un dispositivo real.

图4. spyware 场景的实际训练报告。原文片段；所有数据均为合成。编辑重构；不构成真实证据。

ESCENARIO SINTÉTICO · ZERO BREACH TOOLKIT 2.0.6 · worth-a-look

```
########################################################################
  TRAINING EXAMPLE - NOT A REAL CHECK
  Scenario: worth-a-look. This is a made-up phone checked against made-up
  indicators. It says nothing about this computer or any real device.
########################################################################
========================================================================
  Zero Breach Toolkit 2.0.6 - spyware indicator check
  Scope: default (phone evidence only)
  Checks for TRACES of known mercenary spyware. A clean result is NOT a
  clean bill of health - see what could not be checked, below.
  2026-11-10T18:37:33   Windows 11
========================================================================

========================================================================
  SUMMARY  —  read this part
  TRAINING EXAMPLE: a made-up phone and made-up indicators, not a real check.
========================================================================
  RESULT: no known indicator was found in anything that could be
          checked.

  This is NOT a clean bill of health. See the two sections below for
  what was searched and, more importantly, what could not be.

  ALSO: 4 items under "WORTH A LOOK" further down. They are NOT
  a finding; each comes with its usual, ordinary explanation.

  WHAT COULD NOT BE CHECKED  (4 gaps, grouped)
    - android/android:file-hashes: the collection has no file
      fingerprints (AndroidQF's "hash files" option was off), so files
      were checked by path and name only
    - android/android:history: no battery history in the collection
    - android/android:crashes: bug report missing or unreadable; crash
      records were not checked
    - android/android:messages: no SMS backup in the collection, so
      links in messages were not checked
    (The full report lists them again at its end.)

  Before you share this report: it can contain your Windows username,
  browser profile names, file paths and browsing details, SMS senders
  and message excerpts. --share-json writes a minimal summary without
  artifact text. Ask a responder how to share evidence securely; do
  not post the full report publicly.
========================================================================

Indicator set : 6 indicators, unknown age
  ** WARNING: one or more source dates are unknown; copying files does not refresh indicators. **

DETAIL  —  what was examined, and the evidence behind the summary

--- android-intrusion check  [NOT_APPLICABLE] ---
```

Fragmento literal del reporte real de entrenamiento. No representa un dispositivo real.

图5. worth-a-look 场景的实际训练报告。原文片段；所有数据均为合成。编辑重构；不构成真实证据。

ESCENARIO SINTÉTICO · ZERO BREACH TOOLKIT 2.0.6 · clean

```
########################################################################
  TRAINING EXAMPLE - NOT A REAL CHECK
  Scenario: clean. This is a made-up phone checked against made-up
  indicators. It says nothing about this computer or any real device.
########################################################################
========================================================================
  Zero Breach Toolkit 2.0.6 - spyware indicator check
  Scope: default (phone evidence only)
  Checks for TRACES of known mercenary spyware. A clean result is NOT a
  clean bill of health - see what could not be checked, below.
  2026-11-10T18:37:34   Windows 11
========================================================================

========================================================================
  SUMMARY  —  read this part
  TRAINING EXAMPLE: a made-up phone and made-up indicators, not a real check.
========================================================================
  RESULT: no known indicator was found in anything that could be
          checked.

  This is NOT a clean bill of health. See the two sections below for
  what was searched and, more importantly, what could not be.

  WHAT COULD NOT BE CHECKED  (4 gaps, grouped)
    - android/android:file-hashes: the collection has no file
      fingerprints (AndroidQF's "hash files" option was off), so files
      were checked by path and name only
    - android/android:history: no battery history in the collection
    - android/android:crashes: bug report missing or unreadable; crash
      records were not checked
    - android/android:messages: no SMS backup in the collection, so
      links in messages were not checked
    (The full report lists them again at its end.)

  Before you share this report: it can contain your Windows username,
  browser profile names, file paths and browsing details, SMS senders
  and message excerpts. --share-json writes a minimal summary without
  artifact text. Ask a responder how to share evidence securely; do
  not post the full report publicly.
========================================================================
```

Fragmento literal del reporte real de entrenamiento. No representa un dispositivo real.

图6. clean 场景的实际训练报告。原文片段；所有数据均为合成。编辑重构；不构成真实证据。



ESCENARIO SINTÉTICO · ZERO BREACH TOOLKIT 2.0.6 · cellebrite

```
########################################################################
  TRAINING EXAMPLE - NOT A REAL CHECK
  Scenario: cellebrite. This is a made-up phone checked against made-up
  indicators. It says nothing about this computer or any real device.
########################################################################
========================================================================
  Zero Breach Toolkit 2.0.6 - spyware indicator check
  Scope: default (phone evidence only)
  Checks for TRACES of known mercenary spyware. A clean result is NOT a
  clean bill of health - see what could not be checked, below.
  2026-11-10T18:37:34   Windows 11
========================================================================

========================================================================
  SUMMARY  —  read this part
  TRAINING EXAMPLE: a made-up phone and made-up indicators, not a real check.
========================================================================
  RESULT: SERIOUS FINDING - seek expert help promptly.

  WHAT WAS FOUND
    >> SIGNS THIS PHONE WAS UNLOCKED WITH A PHONE-FORENSICS TOOL (CELLEBRITE)
       cellebrite usb 04f2:b071  [forensic]
          A trace of Cellebrite, the phone-forensics tool police and
          security services use to unlock seized phones and copy their
          contents. It is not spyware: it shows the phone was unlocked, or
          an unlock was attempted, while it was out of its owner's hands.
          the phone's own system logs name it - it may have been a
          connection, a lookup, or only text an app wrote to the log
          Where: phone log logcat.txt, line 2

  WHAT TO DO
    Someone unlocked this phone, or tried to, with Cellebrite: the
    phone-forensics tool police and security services use to copy
    everything on a seized phone. Assume what was on the phone then -
    messages, photos, contacts, saved passwords and the accounts
    signed in - was copied. Change the passwords of important accounts
    from another device, sign out other sessions, and tell the people
    whose conversations were on it. In documented cases spyware was
    installed after such an unlock, so check the apps installed around
    that time and get expert help.

    Seek expert help promptly. Preserve this report and the named
    files or registrations. Do NOT delete, move, run or try to clean
    them. A file match establishes presence; a registration
    establishes configuration. Neither alone establishes that spyware
    executed.

    Contact a qualified incident responder or your organisation's
    security team. You do not need to finish investigating first.
    Support options are at the end of this report.

    Do NOT open, visit or look up indicator addresses. Keep the [.]
    spelling when sharing them.

  WHAT COULD NOT BE CHECKED  (4 gaps, grouped)
    - android/android:file-hashes: the collection has no file
      fingerprints (AndroidQF's "hash files" option was off), so files
      were checked by path and name only
    - android/android:history: no battery history in the collection
    - android/android:crashes: bug report missing or unreadable; crash
      records were not checked
    - android/android:messages: no SMS backup in the collection, so
      links in messages were not checked
    (The full report lists them again at its end.)

  Before you share this report: it can contain your Windows username,
  browser profile names, file paths and browsing details, SMS senders
  and message excerpts. --share-json writes a minimal summary without
  artifact text. Ask a responder how to share evidence securely; do
  not post the full report publicly.
```

Fragmento literal del reporte real de entrenamiento. No representa un dispositivo real.

图7. cellebrite 场景的实际训练报告。原文片段；所有数据均为合成。编辑重构；不构成真实证据。

9. 安全交付给鉴定人或响应团队

9.1 先交摘要，再交完整案卷

发送全部材料前，先询问案件接收人需要什么、通过什么渠道交付。首次沟通可以只涉及担忧原因、设备、范围、日期、结果和缺口。最简摘要便于决定是否需要完整报告，并避免传输无助于回答问题的历史记录或消息。

需要完整报告时，应通过安全渠道交付，而不是作为公开文件发布。工作版本与分享版本应分开。接收人可能需要原始对象，但这一点必须明确约定。不要将 Android 采集数据、iOS 备份或报告上传到陌生服务、聊天群组或通用分析网站。[17]

9.2 用于可验证交付的 Hash 与 EML

如果通过电子邮件发送报告，应保存完整 EML，包括正文、邮件头和附件。正文可以列出每个文件的算法和 hash。接收方自行计算并比较。匹配只能证明文件与该次交付所声明的文件相同，不能证明设备的真实性或发现的正确性。事后计算的 hash 只能证明自计算之时起的完整性。

邮件加密、签名和 hash 解决的是不同问题。加密限制谁能读取；签名有助于核实来源和是否被改动；hash 用于比较对象。三者都不能证明撰写消息的人就是其声称的身份，也不能证明内容真实。不要在同一封邮件中发送私钥或文件密码，应使用另行约定的独立渠道。

对象	记录内容	不能证明什么
交付 EML	正文、邮件头、附件和接收记录。	人类发件人撰写了内容。
TXT / JSON 报告	名称、大小、hash、日期和版本。	范围完整或设备真实。
分享摘要	结果、范围、缺口和下一步。	完整的取证鉴定或不存在风险。
密钥或密码	使用单独渠道并确认接收人。	任意接收者均获得交付授权。
原始采集数据	授权、覆盖范围、保管链和各对象的 hash。	任何工具都能读取所有取证工件。

9.3 避免引发第二次危机的说明

交付案件的简短说明

担忧原因：[观察到的行为和日期]
设备与授权：[类型、所有者和许可]
工具与版本：[来源和验证]
范围：[检查了什么、未检查什么]
结果：[匹配项、参考和缺口]
已采取的操作：[未删除或清理]
交付对象：[摘要 / 报告 / 原始材料]
每个文件的 hash：[算法和值]
我需要：[范围复核、解释和下一步]
未纳入的数据：[密钥、密码、私密或无关内容]

[17] Zero Breach Toolkit。PRIVACY：常规分析在设计上不执行上传；更新与 Android 采集是不同活动。报告可能包含敏感数据，分享摘要不能替代完整报告。 官方在线来源

> **目的不是赢得争论**
>
> 鉴定人不需要当事人证明自己判断正确，而需要来源、时间线和已采取操作的说明。妥善保存的不确定性，比虚构的确定性更有用。

附录A 鉴定人可复现协议

A.1 环境与来源记录

用于生成本指南示例的记录

仓库：`https://github.com/interplains/Zero-Breach-Toolkit`
`Commit: 10ceaba497e40da1f327916a0a3fe0af0ff5994f`
所示版本：`Zero Breach Toolkit 2.0.6`
`JSON` 架构：`1.6`
文件：`scan/zero-breach-toolkit.py`
`SHA-256: 4f7294b0d72ae901552e3ac44f64148c0059d43d587a1638654ab00e7c80e627`
场景：`spyware`、`worth-a-look`、`clean` 和 `cellebrite`
数据类型：完全合成
个人信息：未检查
真实设备：未使用

本记录描述了一次仓库克隆和训练运行；既不是 Windows 可执行文件的构建证明，也不是对最新版本的验证。下载的可执行文件必须针对其自身版本和构建流程进行核查。四个场景均已实际运行并生成 TXT 和 JSON，还生成了一份 `--describe` 的 JSON 输出。

A.2 经授权实际执行的记录表

鉴定记录模板

案件与授权：[标识符、所有者、范围和排除事项]
核查原因：[行为与问题]
设备与初始状态：[型号、系统、日期、时区]
软件包：[仓库、版本、文件和验证]
软件包与指标的 `hash`：[数值和日期]
环境：[分析设备、隔离和同步]
范围：`[default / full / targeted / browser / phone]`
命令与参数：[不含机密]
带时区的开始与结束时间：[原始记录]
输出：`[TXT、JSON、摘要、manifest 和 hash]`
结果与代码：[原文]
发现：[等级、对象、来源和背景]
缺口：[未执行的检查项及原因]
异常：[错误、限制和不可用文件]
证据保存与保管：[位置、访问和转移]
复核：[人员、日期和下一项核查]

A.3 解释矩阵

问题	可回答问题的来源	不能作出的论断
发现了什么?	匹配项、等级和对象。	自动认定感染或攻击者身份。
哪些内容未能检查?	Coverage.not_checked 和 scan_state。	遗漏的位置是干净的。
使用了哪些来源?	指标、版本和日期。	最近的副本就是当前证据。
哪些现象可能正常?	配置、应用和设备所有者的背景。	未经印证就认定误报。
归因还缺什么?	授权、会话、设备和时间线。	仅凭 IP、应用或 MAC 地址认定现实中的个人。
分享什么?	根据需要分享摘要或完整报告。	公开报告是无害的。

验收标准

报告应使他人能够复现范围、定位每项发现、理解每个缺口，并知道哪些事项仍未得到证明。如果只有“干净”或“感染”标签，就还不是完整的复核。

附录B 法律框架、隐私与最终检查

安全检查也涉及个人数据。在墨西哥，适用现行 LFPDPPP 关于目的限制、比例、安全、保密和数据安全事件的规定。秘鲁、智利、阿根廷、哥伦比亚、厄瓜多尔和西班牙 / 欧盟也有最小化、安全、权利和服务提供商方面的等效但不完全相同的规定。在智利，Ley 21.719 的现代化改革推迟至2026年12月1日生效，不得提前将其视为已全面生效的制度。不存在可以读取他人设备的通用授权。[18][19][20][21][22][23][24]

结束前的检查	必须回答的内容
当事人是否安全并获得授权?	未因好奇或未经许可而运行任何测试。

[18]墨西哥。《私营主体持有个人数据联邦保护法》，文本公布于20-03-2025，改革日期为14-11-2025。第5–9、18–20和31条：原则、安全、保密、数据安全事件和权利请求处理。当前联邦主管机构为反腐败与善治部。 官方在线来源

[19]秘鲁。Ley 29733 及其由 DS 016-2024-JUS 批准的条例。目的限制、比例、安全和保密原则；新条例规定了事件、预防性评估和数据官职责的渐进安排。 官方在线来源

[20]智利。Ley 21.719，修订关于个人数据保护的 Ley 19.628。新制度版本推迟至01-12-2026生效；在此之前，应查阅当时适用的规范，不得将未来义务当作现行义务。 官方在线来源

[21]阿根廷。Ley 25.326，更新文本。第4–6、9–10、14–16和25条：质量、信息、安全、保密、数据主体权利，以及代表第三方提供数据处理服务。 官方在线来源

[22]哥伦比亚。Ley Estatutaria 1581 de 2012，第4、8、12、17–18和26条：原则、权利、信息、责任人与处理人的义务，以及向第三国传输。 官方在线来源

[23]厄瓜多尔。《个人数据保护组织法》，Registro Oficial Suplemento 459 de 26-05-2021。第10、37–44条：原则、安全措施、设计即保护、风险及事件发生时的处理。 官方在线来源

[24]欧盟。Reglamento (UE) 2016/679，第5、25、28和32–34条：原则、设计即保护、处理者、安全以及安全事件的通知 / 通报。西班牙还要求审查适用的国内和行业立法。 官方在线来源

结束前的检查	必须回答的内容
软件包是否经过验证?	仓库、版本和来源均有记录。
输出是否得到保护?	本地文件夹，访问和同步均受控。
是否区分了发现、参考和缺口?	未凭标签就认定感染或安全。
是否解释了正常可能，同时未排除严重问题?	配置和背景均已核查。
分享报告时是否落实最小化?	先交摘要；完整案卷通过安全渠道交付。
鉴定人能否复现?	版本、范围、命令、hash、缺口和保管链均已列明。

结语

正确的问题不是“我是不是偏执？”，而是“我能在不造成更多伤害的情况下核实什么？”。答案可能是一项配置、一个巧合、一个缺口或一次专业复核。这些都比没有来源的指控更有用。