ICS 13.310
CCS A92

团 体 标 准

T/GDCIE 005-2025

Tor 暗网网络取证技术要求

Technical Specifications for Tor Network-Based Dark Web Forensics

2025-3-13 发布 2025-3-13 实施

广东省电子学会 发布

目　　次

前　言

本文按照GB/T 1.1-2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件中的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由广州海关缉私局提出。

本文件由广东省电子学会归口。

本文件起草单位：广州海关缉私局、广州大学、广州市公安局电子数据检验鉴定实验室、中移物联网有限公司、奇安信科技集团股份有限公司、华南理工大学、广州锦行网络科技有限公司、广东中法司法鉴定中心、广东司法警官职业学院司法鉴定中心、广东工业大学、华南师范大学、华南农业大学、西安理工大学、江西理工大学、南方医科大学、华中师范大学、湘潭大学、武汉大晟极科技有限公司、深圳市声扬科技有限公司、广州翔越信息科技有限公司、北京宝捷拿科技发展有限公司。

本文件主要起草人：侯文明、刘凯、谭庆丰、胡滨、李志荣、刘宁、王嘉川、吴建亮、于雷、张颖、钟志钊、张靖、张岑锦、毛元惜、曹军、黄文乐、吴鑫杰、冯聪、高坤、高涛、段继平、郑文鑫、刘聪、杨致远、田霄飞、吴鸿华、杨可、秦国栋、孙为军、曾碧卿、张足生、王一川、陈益杉、李本富、王涛、徐金成、邹同浩、周梦麟、刘昊霖、张华军、谢单辉、丁海磊、杨洋、刘星。

本文件为首次发布。

Tor 暗网网络取证技术要求

1 范围

本文件规定了对Tor暗网进行远程数据获取所需设备的技术要求。

本文件适用于对Tor暗网进行远程数据获取的规范化操作。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 29360 法庭科学电子数据恢复检验规程

GA/T 1476-2018 法庭科学远程主机数据获取技术规范

GA/T 1478-2018 法庭科学网站数据获取技术规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

洋葱路由 Tor（The Onion Router）

Tor 是实现匿名通信的自由软件。

3.2

Tor 浏览器 Tor Browser

安装在计算机、手机、智能设备等终端上用于访问 Tor 暗网的客户端程序。

3.3

暗网 Dark Web

暗网是构建在公共 Internet 之上，使用非常规协议和端口以及可信节点进行连接的私有网络，需要专门的软件、配置或者认证才能访问的网络，具有匿名性强、溯源难、动态性高等特点。

3.4

Tor 暗网 Tor Network-Based Dark Web

Tor 暗网是指架构在 Tor 网络之上，使用顶级域后缀.onion 和洋葱路由技术的一种暗网。

3.5

Tor 隐藏服务描述符 Tor Hidden Service Descriptor

用户维护 Tor 隐藏服务的元数据，如时间戳、编码方式、加密公钥等。

4 总体原则

4.1 全面性原则：数据获取结果宜覆盖要求中的所有相关数据。

4.2 可控性原则：对 Tor 暗网所进行的任何篡改（包括权限提升、渗透等）都应进行风险评估。

4.3 可追溯性原则：应及时、客观、全面地记录与数据获取有关的操作，对不可再现情况的录像记录，应确保数据获取过程和结果的可追溯性。

4.4 可靠性原则：用于数据获取的设备，应经过核查，并定期进行更新和维护，以确保数据获取结果准确可靠。

5 设备

5.1 Tor 暗网网络数据获取使用的设备在基础访问方面应具备的功能：

a）支持登录 Tor 浏览器访问 Tor 暗网；

b）支持 Tor 暗网数据获取，如获取网站元数据、网页数据；

c）支持 Tor 暗网隐藏服务描述符数据获取。

5.2 Tor 暗网网络数据获取使用的设备在关系分析和服务器数据获取方面宜具备的功能：

a）支持网络拓扑关系建立和分析；

b）支持利用 Tor 暗网特定字段建立用户和暗网之间的关联关系；

c）支持对 Tor 暗网网站所在服务器端数据（如服务端操作系统、后台数据库、网络数据报文、网站指纹等）的提取和恢复。

d）支持远程数据获取，如对远程目标站点内容自动抓取、录屏和网页截屏操作。

6 数据获取过程

6.1 数据获取准备

a）了解 Tor 暗网访问过程及通信方式；

b）宜了解 Tor 暗网访问关系（如访问、浏览等），并从访问关系中的其他方获取电子数据副本；

c）记录数据获取对象相关情况，如 Tor 暗网域名、Tor 暗网网站的基本信息；

d）准备相应的数据获取设备，搭建数据获取环境。

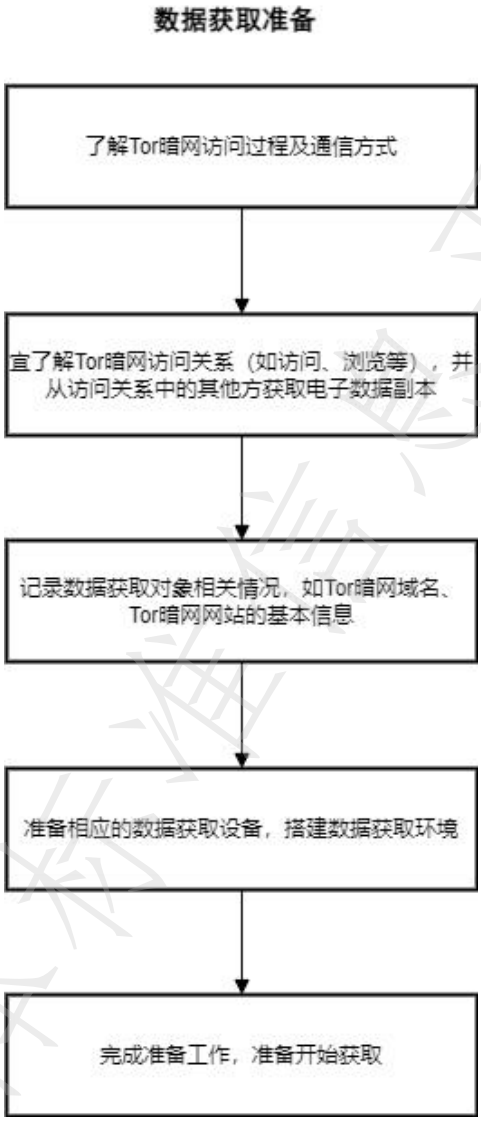

图 1 数据获取准备过程图

6.2 数据获取

6.2.1 对于 Tor 暗网网站，应按照以下步骤提取、固定暗网网页及其他相关文件：

a）使用屏幕录像软件启动屏幕录制，或使用摄像机拍摄屏幕显示内容；

b）与国家授时中心等标准时间源进行时间校对，记录准确的开始时间；

c）访问 Tor 暗网网站，查看暗网网站基本信息，并对暗网网页进行搜索、提取、固定，必要时可使用网络数据包捕获的方式进行数据获取；

d）如有条件，可对 Tor 暗网域名信息或 Tor 暗网网站所在的服务器进行网络溯源；

e）如有条件，可对 Tor 暗网网站所在服务器、后台数据库、日志记录等内容进行提取固定；

f）计算提取和固定的 Tor 暗网网页、文件的完整性校验值；

g）再次进行时间校对，记录准确的结束时间，结束屏幕录制或摄像机拍摄。

6.2.2 提取固定过程中不应删除、修改 Tor 暗网网页，或执行其他可能影响 Tor 暗网网站客观性的操作。

6.2.3 应计算提取固定过程录像的完整性校验值。

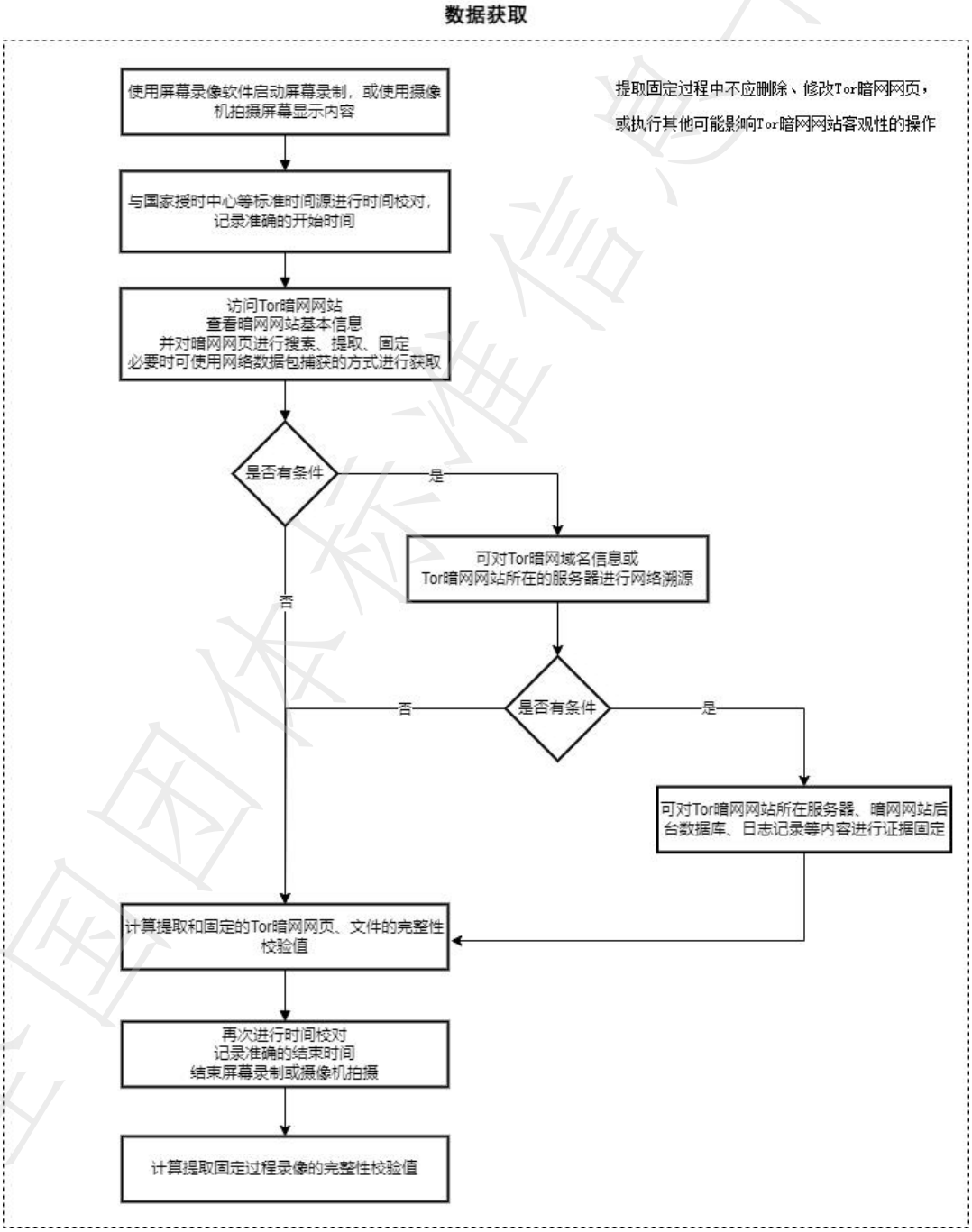

图 2 数据获取过程图

6.3 电子数据分析

Tor 暗网电子数据的分析包括存在性分析和真实性分析。

6.3.1 存在性分析

电子数据存在性分析，包括但不限于以下内容：

a）暗网网站域名及其存活性；

b）暗网网站目录结构、文件格式和属性；

c）暗网网站采用的开发框架和中间件；

d）提取固定文件的内容和属性。

6.3.2 真实性分析

数据真实性分析，包括但不限于以下内容：

a）应分析 Tor 暗网网站中的网页内容、网站框架、结构和代码的同源性；

b）应分析 Tor 暗网网站中的图片、文档、压缩包等文件的来源，及与暗网用户之间的关联关系；

c）应分析 Tor 暗网网络流量、访问日志、通联关系、数字货币地址和实体；

d）宜分析 Tor 暗网网站后台数据库、日志、已恢复的删除数据及数据之间的关联性。

参 考 文 献

[1] 《匿名通信与暗网》谭庆丰、时金桥、王学宾著，科学出版社，2019年10月
[2] 《匿名通信技术研究》王丽宏著，人民邮电出版社，2020年11月