Computer Science and Application 计算机科学与应用, 2026, 16(9), 224-235
Published Online September 2026 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2026.169303

Hans汉斯

家庭路由器镜像提取分析研究

何　宇[1]，鲍梦湖[2*]，郝鹏程[1]，孙善为[3]

[1]西安市公安司法鉴定中心，陕西　西安
[2]公安部鉴定中心，痕迹科学与技术公安部重点实验室，北京
[3]国投智能信息科技股份有限公司，福建　厦门

收稿日期：2026年8月12日；录用日期：2026年9月15日；发布日期：2026年9月22日

摘　要

家庭路由器作为室内现场最常见的电子设备，记录着网络访问记录、设备连接日志等关键的涉案线索，是重要的电子数据取证工作对象。本文以家庭路由器为研究对象，尝试通过多种方式提取路由器存储镜像文件并进行解析。研究结果表明，相较于传统家庭路由器Web取证方式，使用镜像提取解析的方式不但能部分绕过密码限制，还可以提取到更多的网络访问日志、设备连接记录等信息。

关键词

家庭路由器，镜像提取，电子数据提取

Research on Image Extraction and Analysis of Home Routers

Yu He[1], Menghu Bao[2*], Pengcheng Hao[1], Shanwei Sun[3]

[1]Forensic Science of Xi'an Public Security Bureau, Xi'an Shaanxi
[2]Ministry of Public Security & MPS' Key Laboratory of Forensic Marks, Institute of Forensic Science, Beijing
[3]SDIC Intelligence Information Technology Co., Ltd., Xiamen Fujian

Received: August 12, 2026; accepted: September 15, 2026; published: September 22, 2026

Abstract

As the most common electronic equipment at indoor crime scenes, home routers store critical case-related clues including network access records and device connection logs, making them vital targets for electronic data forensics. Taking home routers as the research object, this paper explores multiple methods to extract and analyze router storage image files. The research results demonstrate that compared with the traditional Web-based forensics method for home routers, image

*通讯作者。

文章引用: 何宇, 鲍梦湖, 郝鹏程, 孙善为. 家庭路由器镜像提取分析研究[J]. 计算机科学与应用, 2026, 16(9): 224-235. DOI: 10.12677/csa.2026.169303

extraction and analysis can partially bypass password restrictions and retrieve more data such as network access logs and device connection records.

Keywords

Home Router, Image Extraction, Electronic Data Acquisition

1. 引言

在信息化时代，互联网已全面融入家庭生活，家庭路由器作为家庭网络连接核心设备，承担着终端设备联网的核心功能，也使其成为室内案件现场勘查工作中重点的勘查取证目标。家庭路由器内部存储的联网设备列表、网络访问日志、端口转发记录、WiFi 连接记录、流量使用记录等数据，能够还原涉案人员的网络行为轨迹，为案件侦破、事实认定提供关键电子证据。

在实际工作中，针对家庭路由器的取证方式仍以传统 Web 页面取证方式为主，取证人员通过浏览器登录路由器后台管理界面，调取设备基础信息、在线设备列表、简易日志等数据。但 Web 端取证的方式存在很大局限，家庭路由器厂商为保障设备运行安全与用户隐私，对 Web 后台权限进行了严格限制，仅开放浅层、非核心数据的查询权限，大量深层系统数据、临时运行数据、日志记录等数据无法通过 Web 界面获取。

为进一步挖掘家庭路由器中的涉案电子数据，本文尝试对路由器设备闪存数据、内存运行数据进行镜像提取与解析，梳理不同的镜像提取方法的操作流程、技术要点与适用场景，对比不同取证技术的优劣，总结取证实践中的难点与优化策略，旨在为家庭路由器电子取证工作提供更多的技术方案。

2. 家庭路由器概述

家庭路由器一般是指用于连接家庭或其他小型场景下网络互联的计算机专用设备[1]，它可以通过提供无线热点等方式，为终端设备(如手机、笔记本电脑)提供互联网接入服务。家用路由器的主要功能包括网络互联、数据处理、网络管理等[2]。

2.1. 家庭路由器与工业路由器的区别

工业路由器面向生产等专业场景，以长期稳定运行、可方便运维为设计目标，配备 Console 调试接口、保留多类日志和连接信息；而家用路由器受成本限制，基本不保留调试接口，无独立临时存储，安全策略固定不可调，仅能查看简易实时联网日志，设备断电即丢失临时操作痕迹。

2.2. 家庭路由器操作系统(固件)类型

主流家用路由器操作系统底层均以嵌入式 Linux 系统为基础，路由器厂商依据自己的硬件开发适配的固件[2]，如 Vxworks、ASUSWRT 等闭源操作系统。此外，近年来以 OpenWrt、Tomato、Merlin 为代表的开源第三方路由器固件应用也越来越普及，这些操作系统可进行自定义开发，而非简单的只读固件；且操作系统底层数据开放，插件生态丰富，受网络技术爱好者与科研人员青睐。

2.3. 家庭路由器核心存储芯片介绍

家庭路由器的核心存储芯片主要有随机存取存储器(RAM)和闪存存储器(FLASH)两类，分别存放路由器系统数据、运行数据、用户配置数据、日志数据等。

RAM 芯片即路由器内存，属于易失性存储硬件，主要用于路由器运行过程中的系统程序加载、数据缓存、临时运算存储。路由器加电运行时，RAM 会实时加载系统内核、运行进程、联网状态、终端连接信息、实时操作痕迹等临时数据。但 RAM 芯片不具备断电留存能力，设备一旦断电、重启，内部所有临时数据会彻底清空，无法恢复。家庭路由器 RAM 芯片容量普遍较小，仅能满足设备基础运行需求，无多余空间留存历史缓存数据。

FLASH 芯片即路由器闪存，属于非易失性存储硬件，是路由器中持久化存储单元，断电后数据不会丢失。FLASH 芯片主要存储路由器系统固件、配置文件、WIFI 密码、联网账号、设备绑定信息、系统日志等核心固化数据，是路由器静态取证的核心对象。家庭路由器 FLASH 芯片容量普遍在 8 MB~128 MB，FLASH 芯片数据可通过物理拆机、芯片读取、软件抓取等多种方式提取，是路由器镜像取证的主要研究对象(见图 1)。

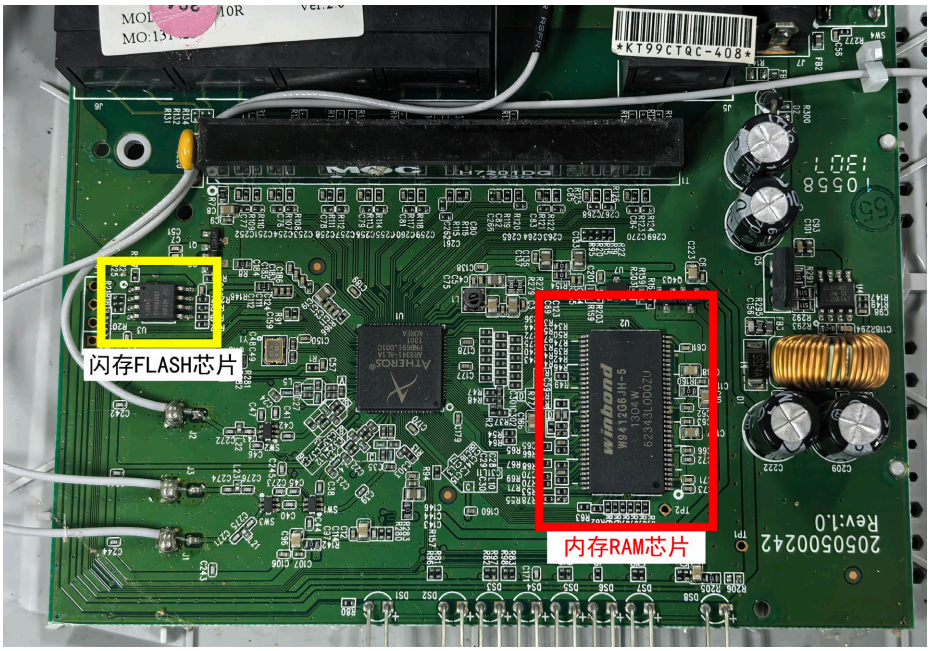

Figure 1. Storage chip appearance on router main-boards
图 1. 路由器主板上存储芯片样式

3. 家庭路由器镜像提取方法研究

结合家庭路由器的硬件特性与取证实践，本研究计划使用 UART(TTL)提取、SSH 提取、FLASH 芯片物理提取、Console 提取、JTAG 提取等方法对家庭路由器存储芯片镜像进行提取。

3.1. TTL 电平的 UART 接口连接提取镜像

UART (Universal Asynchronous Receiver/Transmitter)调试接口按照电平标准分为 TTL、和 RS-232 等，路由器上多预留 TTL 四针焊盘(TX/RX/GND/VCC) (见图 2)作为底层控制台，因此本研究采用 TTL 电平的 UART 接口进行取证。

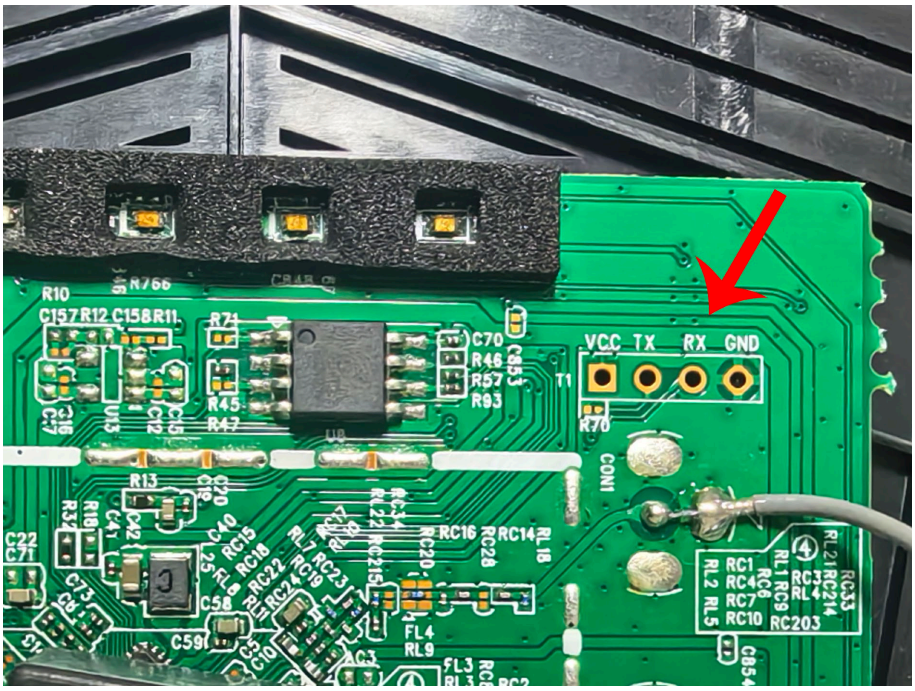

Figure 2. TTL pad appearance on router main-boards
图 2. 路由器主板上 TTL 焊盘样式

首先需拆卸路由器外壳(尽量不要断电)；找到主板上的 TTL 调试接口，使用万用表根据电压不同分别测出 VCC、TX、RX、GND 四个针脚；使用夹具及 USB 转 TTL 烧录器连接路由器 TTL 焊盘和取证计算机；连接完成后，保持路由器加电运行状态，通过串口调试工具(本研究使用 SecureCRT)配置波特率、数据位、校验位等参数，建立稳定的通信连接。连接成功后，使用命令查看路由器账号和密码(见图 3)，读取并 dump 路由器内存和 Flash 闪存镜像并保存至取证计算机，完成镜像提取。

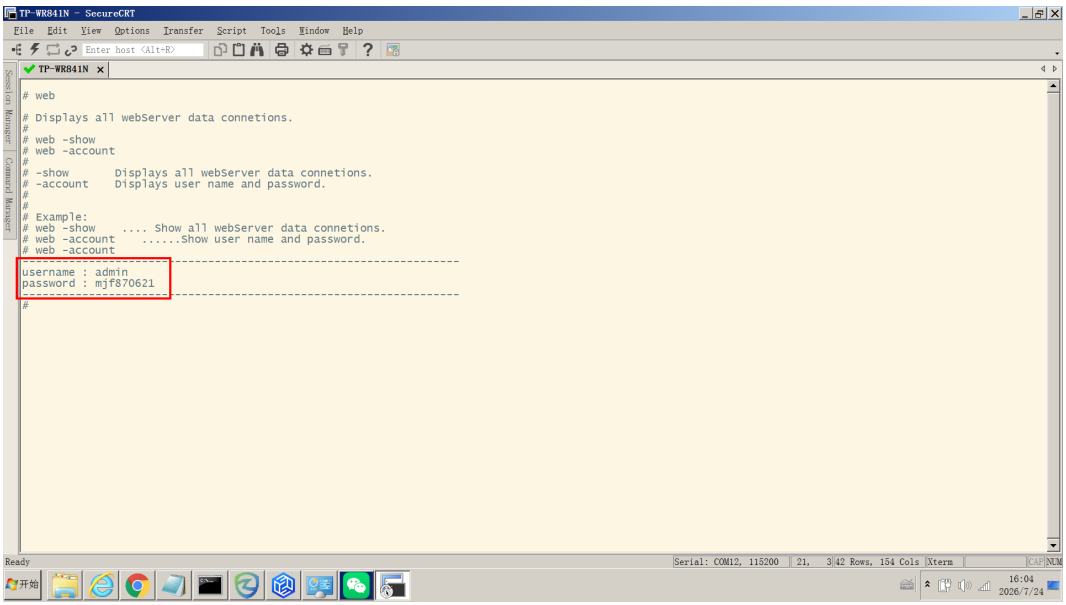

Figure 3. Viewing router accounts and passwords via web commands
图 3. 使用 web 命令查看路由器账号和密码

此类方式提取镜像不需要路由器账号密码信息。但实验发现，为了系统安全，路由器厂商大多采用限制底层读取权限、增加校验锁、限制导出二进制文件大小等方式对闭源固件进行保护。实验发现，对新款路由器无法使用这种方式提取镜像。

3.2. SSH 镜像提取方法

家庭路由器系统多基于嵌入式 Linux 系统开发，大部分路由器固件默认搭载 SSH 服务，因此可以通过网线连接路由器，通过 SSH 工具远程登录设备后台，获取路由器 root 权限后，通过系统指令读取 FLASH 分区数据、内存运行数据，打包生成镜像文件并传输至取证计算机。

首先需将路由器与取证计算机用网线连接，将计算机设置为与路由器相同网段；借助 SSH 工具(本研究使用 MobaXtem 工具)远程连接，输入账号密码完成权限验证(见图 4)。登录成功后，通过指令查看设备存储分区，执行数据读取、打包、导出操作，完成镜像提取(见图 5)。

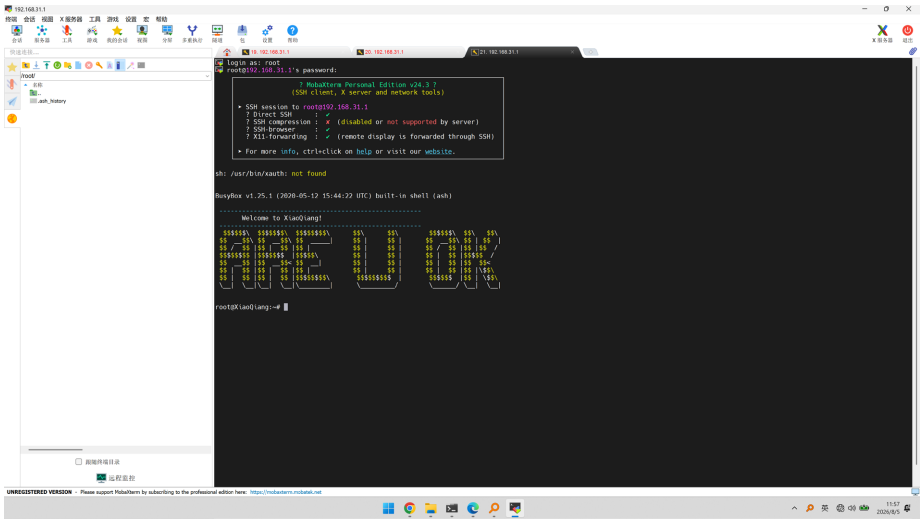

Figure 4. Connect to the router using SSH
图 4. 使用 SSH 连接路由器

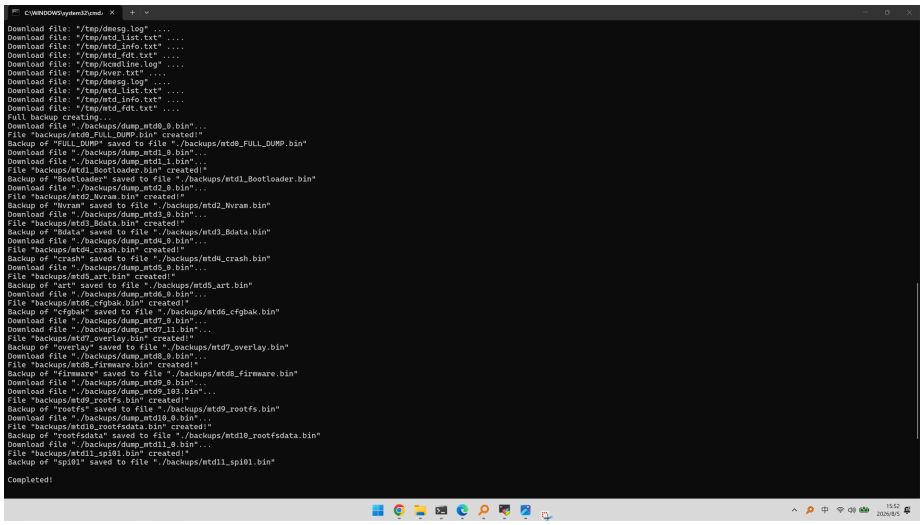

Figure 5. Extracting router image
图 5. 提取路由器镜像

该方法的局限性较为明显，大部分路由器都默认关闭 SSH 服务，且 Web 端不设置手动开启权限。部分路由器虽然开放 SSH 权限，但权限等级较低，无法读取底层核心数据，仅能获取部分基础配置信息，因此需要采用技术手段获取系统最高管理权限后方可提取全量数据。

3.3. FLASH 芯片物理提取镜像方法

FLASH 芯片物理提取是针对路由器提取存储数据的终极取证方法，直接以路由器 FLASH 存储芯片为取证对象，通过免拆机或拆机方式读取芯片全量数据，彻底摆脱系统权限的限制，是最彻底、最稳定的镜像提取方法。芯片物理提取方法主要分为免拆机提取与拆机提取两种模式。

3.3.1. 免拆机提取

FLASH 芯片免拆机提取依托专业芯片读取夹具，无需拆卸芯片，直接贴合路由器主板上的 FLASH 芯片引脚，通过编程器建立数据连接，读取芯片内部所有存储数据，生成镜像文件[3]。该方法无需焊接、拆卸芯片，无硬件损伤，操作便捷、取证效率高，适用于芯片引脚完好、无遮挡、可贴合夹具的路由器设备。

3.3.2. 拆机提取

FLASH 芯片拆机提取为备用方案，当路由器主板布局紧凑、芯片遮挡严重、夹具无法贴合，或芯片引脚氧化、接触不良时，需通过焊台将 FLASH 芯片从主板上拆卸，清理芯片引脚焊锡后，将芯片固定于专用编程器上，完成全量数据读取(见图 6)。

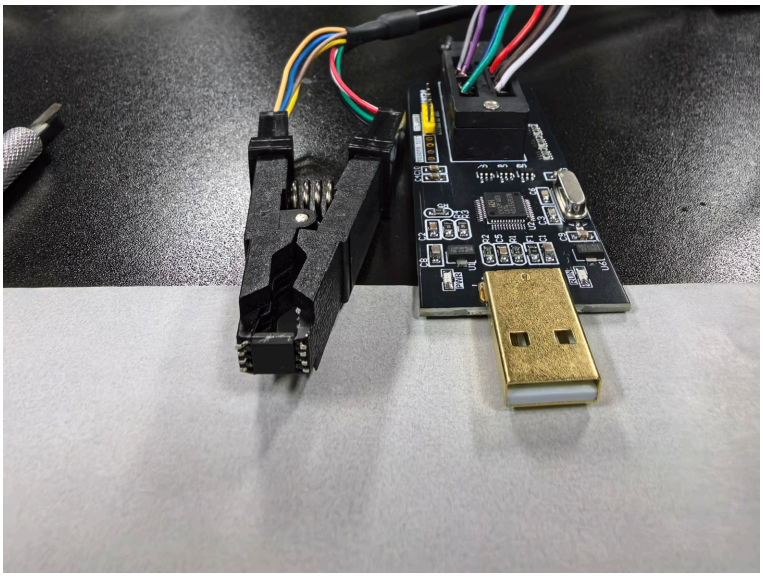

Figure 6. Extracting router FLASH data with XTW-5 programmer
图 6. 使用 XTW-5 编程器提取路由器 FLASH 闪存数据

该方法适配所有带独立 FLASH 芯片的路由器设备，取证兼容性极强，但操作难度高，存在芯片烧毁、引脚损坏的风险，属于破坏性取证方式，仅在其他取证方法失效时使用。

3.4. Console 接口和 JTAG 接口提取镜像方法

Console 接口是专业网络设备的调试接口，广泛应用于工业路由器、交换机、服务器等设备的调试与数据读取。从硬件配置来看，家庭路由器为控制成本、精简结构，基本不再标配 Console 接口，因此无法

通过该方式开展镜像取证研究。

JTAG 接口是芯片级调试接口，主要用于芯片程序烧录、硬件调试、底层数据读取，可直接对接路由器主控芯片，读取芯片内部存储的全量数据，能够获取其他方法无法读取的底层隐藏数据。该方法的核心优势是不受系统固件权限限制，即使路由器系统加密、权限锁定，只要硬件接口正常，就可完成数据提取。

拆开路由器外壳，在路由器线路板上寻找 JTAG 引脚(常见有 4 种：10PIN、14PIN、16PIN、20PIN)(见图 7)；使用嵌入式硬件探测工具(本研究使用 JTAGulator 工具)扫描确定引脚功能；使用仿真器(本研究使用 JTAG/SWD ARM 仿真器)连接 JTAG 引脚，完整 dump 路由器 Flash 固件(见图 8)。

Figure 7. 10PIN JTAG pins on router main-board
图 7. 路由器主板 10PIN 规格 JTAG 引脚

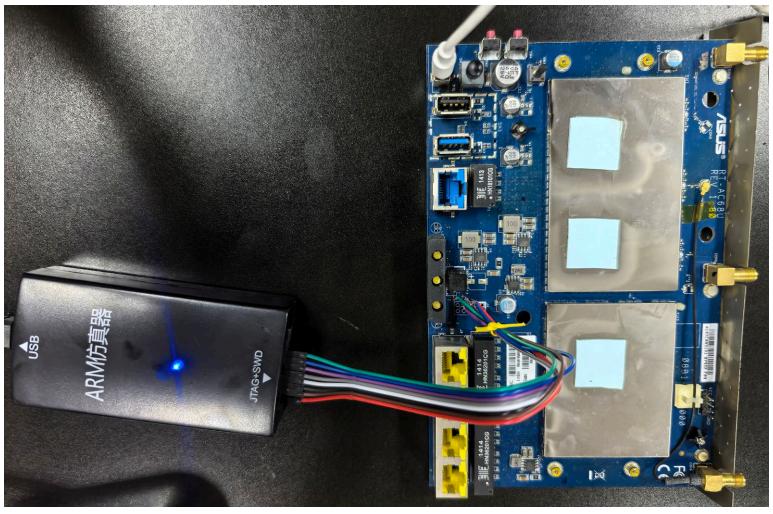

Figure 8. Performing chip extraction by connecting an ARM emulator
图 8. 连接 ARM 仿真器进行芯片提取

绝大多数新款家用路由器厂商会屏蔽或熔断 JTAG 调试引脚，仅少数老旧机型保留该引脚。因此，依靠 JTAG 提取镜像的方案较少使用，不是通用的镜像取证方法。

3.5. 软路由镜像提取方法

软路由是基于计算机、虚拟机搭建的虚拟化路由设备，无专用硬件芯片，依托计算机操作系统实现网络转发、路由管控功能。其镜像提取方式与实体路由器完全不同，提取方式更为简单。软路由本质为虚拟机系统，所有路由数据、配置信息、联网痕迹均存储于虚拟机磁盘文件中，无需拆机、无需对接硬件接口。

其核心取证方法为虚拟机镜像打包技术，可以直接通过虚拟机管理工具，对软路由的系统磁盘、数据磁盘进行完整镜像备份，生成标准化磁盘镜像文件，一次性留存软路由系统全量数据。此外，通过虚拟机快照、内存镜像工具，抓取软路由的实时运行内存数据，获取易失性操作痕迹[4] (见图 9)。

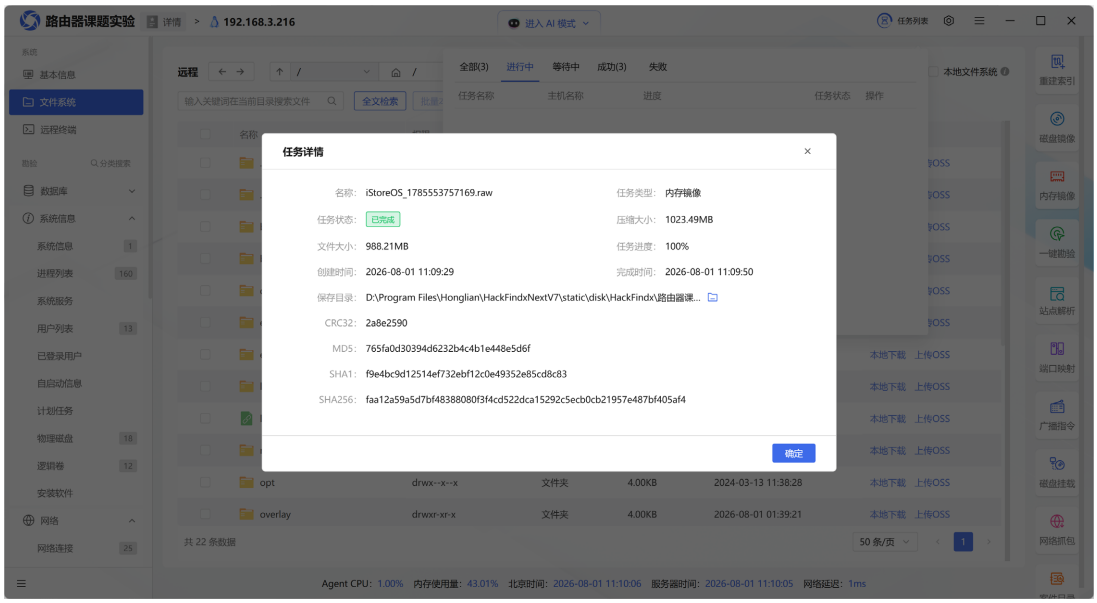

Figure 9. Extracting memory image of the soft router
图 9. 提取软路由内存镜像

整体来看，软路由镜像提取操作简单、数据完整性好，提取难度远低于实体家庭路由器，且无硬件损坏风险，取证流程标准化程度高。

4. 家庭路由器镜像解析方法

常用的镜像取证常用工具包括 Binwalk、FTK Imager、Volatility3 及“物联网取证大师”等一体化取证软件。各类工具功能定位不同，相互配合可实现镜像数据的全方位解析。结合各类工具的功能特性，本研究整理出一套完整的家庭路由器镜像解析流程，涵盖固件镜像解析、内存镜像解析、日志数据分析三大模块，同时适配硬件路由器与软路由取证需求。

4.1. 证据固定与校验

将提取的镜像文件导入取证计算机，计算镜像文件哈希值，同时对镜像文件进行完整性校验，确认提取数据无缺失、无损坏。

4.2. 固件镜像解析

使用 Binwalk 工具对 bin 格式固件镜像进行扫描分析，识别固件分区结构，解压提取系统文件、配置

文件、用户数据文件。通过工具指令筛选 WiFi 配置信息、联网账号、绑定设备信息、端口转发记录、后台登录日志等核心数据，还原路由器基础配置与长期运行痕迹。针对软路由磁盘镜像，直接通过 FTK Imager 完成镜像挂载与文件提取，读取系统配置与历史运行数据。

4.3. 内存镜像解析

采用 Volatility3 工具加载路由器内存镜像文件，开展内存数据解析，梳理设备运行进程、实时网络连接、终端设备接入记录、临时操作指令、缓存访问痕迹等易失性数据，补充固件镜像的取证短板。

4.4. 日志数据整理分析

日志数据主要记录了路由器的启动情况(激活了哪些服务等)、IP 地址分配情况、功能设置情况、网络连接情况、地址认证情况等[5]。使用文本解析工具对系统日志、访问日志、设备日志进行筛选、去重、溯源，通过日志时间轴还原设备联网行为、终端接入行为、后台操作行为，梳理时间节点的关键联网行为。

5. 分析与总结

5.1. 各类镜像提取方法综合对比分析

通过对前文 5 种家庭路由器镜像提取方法的实操特性、取证效果、适配场景、操作难度、设备损伤风险进行系统性对比，整理出各类方法的差异(见表 1)。

Table 1. Comparison of different router image-acquisition methods
表 1. 路由器不同镜像提取方法比对表

提取方法	是否需拆机	是否需断电	是否需账号密码	能否提取内存数据	是否需要解锁
TTL	是	否(部分)	否	是(部分)	是
SSH	否	否	是	是(部分)	是
JTAG	是	是	否	否	否
芯片物理提取	是	是	否	否	否
软路由	否	否	否	是	否

TTL 调试方式需连接电路板测试点即可实现底层数据导出，通用性较强，但大部分设备存在 U-Boot 密码、系统读取权限封锁导致取出数据有限。SSH 依托网络服务开展在线提取，无需拆解设备，但受固件权限策略限制，大部分家庭路由器厂商默认关闭 SSH 服务，若采用此方法提取，首先应先对路由器解锁，操作难度较大。JTAG 方式能够绕过软件权限限制实现芯片级数据读取，但新款设备常熔断调试引脚，普适性不足。芯片物理提取方法通过编程器直接读取闪存芯片原始数据，不受系统、调试接口限制，数据提取可靠性最高，缺点是只能提取 FLASH 闪存芯片数据，无法提取内存数据；且需要拆焊芯片，操作难度大，操作不当易造成芯片损毁。

5.2. 总结

5.2.1. 镜像取证与传统 Web 取证的对比

路由器 Web 取证依托网页管理界面开展数据调取，操作简单、无需拆机，但仅能够获取界面开放的有限信息，无法获取完整的日志信息、网络连接信息等。镜像取证通过 SSH、TTL、JTAG、芯片物体提取等方式获取能够提取到 Web 方式所无法提取的底层原始电子数据，不仅包含用户网络配置信息，还可

提取网络连接记录、日志信息等关键线索。对于部分家庭路由器设备，还可以直接获取路由器账号密码信息，因此在非正常死亡案件等无法获取路由器账号密码信息的案件中能够发挥重要作用。但镜像取证通常需要拆机操作，技术门槛更高，部分提取手段存在硬件损毁风险，后续还需借助二进制分析工具或专用物联网取证软件进行镜像解析。

以小米 AC2350 (内部型号 R2350)为例，通过路由器 Web 管理界面，可获取路由器型号、MAC 地址、设备序列号、WiFi SSID 及密钥等基础配置信息。对于取证所关注的设备连接记录，在 Web 管理界面仅展示当前在线设备的型号、IP 地址与 MAC 地址信息(见图 10)；无法提取设备历史连接记录及系统日志信息。

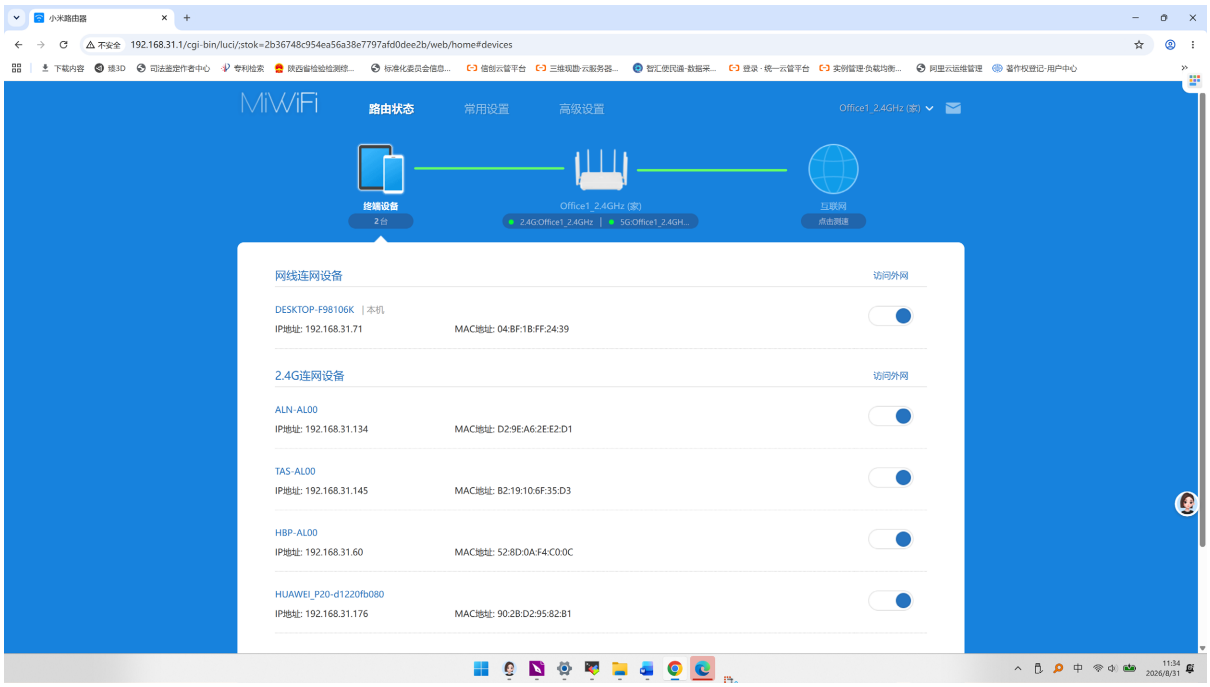

Figure 10. Extracting data via the Web-management interface of Xiaomi AC2350 router
图 10. 小米 AC2350 路由器 Web 管理界面提取数据

以 SSH 方式提取路由器存储镜像，使用 WinHex、FTK Imager 等工具加载镜像文件进行分析。加载镜像文件并浏览路由器文件系统。对文件系统逐一进行搜索，发现设备连接记录、路由器日志记录等信息(见表 2)。

Table 2. Overview of information extracted via image-based forensics
表 2. 镜像取证方式提取信息一览

提取信息	WiFi 账密信息	设备连接记录	路由表	路由器运行日志信息
文件位置	/etc/config/wireless	/etc/xqDb	/rom/etc/config/network	/data/usr/log/messages

对提取内容进行分析，设备连接记录表(xqDb 文件)中包括在线设备和离线设备的型号、IP 地址和 MAC 地址信息。路由器运行日志记录(messages 文件)中详细记录路由器运行、接口调用、报错返回、账号登录等信息，可作为路由器漏洞分析、入侵研判的分析依据(见图 11)。

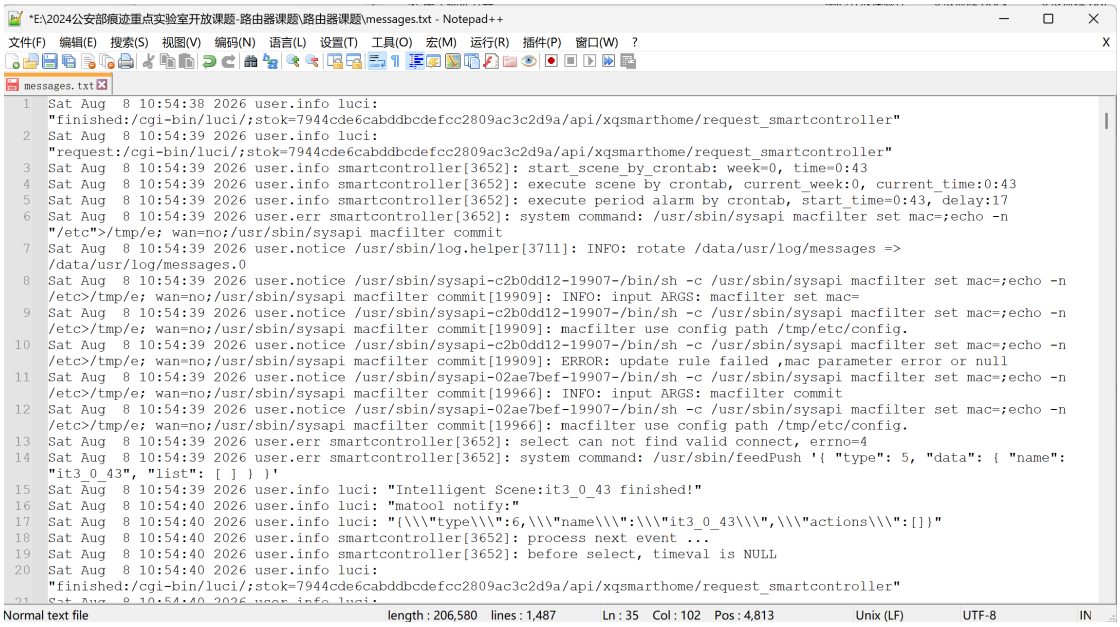

Figure 11. Run-time logs of Xiaomi AC2350 router
图 11. 小米 AC2350 路由器运行日志

5.2.2. 当前路由器取证的核心难点

随着网络安全技术迭代，路由器厂商的安全防护策略持续升级，家庭路由器镜像取证难度不断提升，成为当前取证工作的核心痛点。主流华为、荣耀、小米等品牌新款家庭路由器，均搭载自研加密固件系统，对 FLASH 存储数据、固件镜像进行多层加密封装，即使通过硬件手段成功提取完整的镜像文件，使用现有解析工具也无法破解加密分区、读取底层数据，出现“可提取、不可解析”的取证困境。同时，新款路由器普遍屏蔽 SSH、JTAG 调试权限，精简硬件调试接口，从硬件与软件双层限制底层数据读取，大幅提升了取证难度。

5.2.3. 路由器取证展望

通过路由器镜像取证研究可知，同智能手机设备类似，路由器厂商的安全防护机制持续迭代升级，导致充分提取电子数据的难度不断加大。这就要求电子数据取证人员树立长期学习的理念，借助各类专业技术渠道掌握最先进的电子数据取证技术，并积极转化为实践。针对特定型号路由器公开的调试手段、破解工具，在完成有效性与安全性验证后，就可以运用于案件勘验工作中。信息技术发展日新月异，取证人员必须持续更新知识储备，才能持续应对新型物联网设备不断升级的安全壁垒。

6. 结论

研究表明，对家庭路由器镜像提取取证能够一定程度上补充 Web 方式取证的权限限制与数据短板，提升电子数据提取的全面性，具备较高的案件应用价值。但同时，主流品牌路由器安全策略的持续升级，使得固件加密、权限封锁成为当前取证工作的主要难题，新型设备镜像取证难度也越来越大。未来，需持续深耕物联网设备取证技术，不断提升物联网设备电子数据提取的专业能力，为各类案件的侦查取证提供更坚实的技术支撑。

基金项目

2024 年痕迹科学与技术公安部重点实验室开放课题项目(2024FMKFKT10)。

参考文献

[1] 朱拓, 徐志超. 家用路由器取证方法研究[J]. 信息系统工程, 2021(2): 100-101.

[2] 袁心宇, 张璇, 潘光诚, 等. 家用路由器电子数据取证方法[J]. 刑事技术, 2020, 45(3): 278-283.

[3] 林雄. 智能路由器固件的编译及烧写[J]. 电脑编程技巧与维护, 2017(19): 25-28.

[4] 计超豪, 邱殿聪, 王即墨, 等. 智能路由器数据取证方法[J]. 刑事技术, 2019, 44(5): 447-450.

[5] 韩马剑. 路由器取证研究[J]. 信息网络安全, 2016(9): 51-55.