引用格式： 卓圣钧，黄林轶，赖怡聪，等.基于 Windows 系统的智能健康产品信息安全检测技术研究[J].标准科学，2025(10):107-113.
ZHUO Shengjun,HUANG Linyi,LAI Yicong,et al. Research on Information Security Detection Technology of Medical Equipment Based on Windows System [J].Standard Science,2025(10):107-113.

基于 Windows 系统的智能健康产品信息安全检测技术研究

卓圣钧[1,2] 黄林轶[1,2*] 赖怡聪[1,2] 古晓娥[1,2]
（1.工业和信息化部电子第五研究所；2.智能产品质量评价与可靠性保障技术工业和信息化部重点实验室）

摘 要：【目的】针对智能健康产品的信息安全问题，研究基于Windows系统的智能健康产品信息安全检测技术。【方法】依据智能健康产品信息安全法规与标准，结合实际案例，提出基于Windows系统的智能健康产品及其客户端/服务端架构软件的检测方法。【结果】分析了基于Windows系统的智能健康产品面临的安全挑战，包括近源攻击风险、数据安全风险、网络传输风险等，并验证了所提检测方法的有效性。【结论】所述检测方法可为相关测试工作提供实践指导与技术参考，助力提升运行Windows系统的智能健康产品的信息安全水平，推动医疗行业的数字化安全发展。

关键词： 智能健康产品；Windows操作系统；客户端/服务端架构；法规与标准；信息安全检测
DOI编码： 10.3969/j.issn.1674-5698.2025.10.015

Research on Information Security Detection Technology of Medical Equipment Based on Windows System

ZHUO Shengjun[1,2] HUANG Linyi[1,2*] LAI Yicong[1,2] GU Xiao'e[1,2]
(1.The No.5 Institute of Electronics, Ministry of Industry and Information Technology; 2. Key Laboratory of Intelligent Product Quality Evaluation and Reliability Assurance Technology, Ministry of Industry and Information Technology)

Abstract: [Objective] The paper aims to study the information security detection technology of medical equipment based on the Windows system. [Methods] Detection methods targeting medical equipment running on Windows systems and its Client/Server architecture software are introduced, in line with relevant regulations and standards for medical equipment information security and real cases. [Results] The security challenges faced by medical equipment based on the Windows system are analyzed, including near-source attack risks, data security risks, and network transmission risks, and the effectiveness of the proposed detection methods is verified. [Conclusion] The detection methods mentioned above can provide practical guidance and technical references for related testing work, help enhance the information security level of medical equipment running on the Windows system, and promote the digital and safe development of the medical industry.

Keywords: medical equipment; Windows operating system; Client/Server architecture; regulations and standards; information security detection

---

基金项目： 本文受国家重点研发计划NQI专项（项目编号：2022YFF0607100）课题四（课题编号：2022YFF0607104）资助。
作者简介： 卓圣钧，本科，助理工程师，研究方向为智能产品信息安全。
黄林轶，通信作者，硕士，高级工程师，研究方向为智能产品质量安全。
赖怡聪，本科，助理工程师，研究方向为智能产品信息安全。
古晓娥，本科，助理工程师，研究方向为智能产品信息安全。

0　引 言

在医疗行业数字化转型浪潮中，智能健康产品的信息安全状况直接关系到患者隐私安全、医疗服务质量乃至生命安全。然而，在智能健康产品开发进程中，开发人员往往将主要精力集中于设备功能的完善及操作便捷性的提升，对信息安全防护设计这一关键环节投入的关注度相对不足，导致设备在投入应用之初即存在固有安全缺陷[1-3]。在实际使用中，弱口令、随意接入USB设备及操作系统版本老旧等问题使设备极易感染勒索病毒，面临严重安全威胁[4-5]。因此，相关检测技术的研究成为众多学者和机构关注的焦点。在操作系统层面，可采用弱口令检测、端口扫描、配置文件与数据库检查等方法进行测试[6]。针对客户端/服务端（Client/Server，C/S）架构软件，客户端检测可运用程序加壳检测、签名校验、动态调试、TCP协议抓包等分析方法，有效识别该架构软件的常见漏洞。

尽管如此，对于高度定制的C/S架构软件与多样化的Windows系统版本深度集成的这类智能健康产品的信息安全检测工作，仍面临诸多困难与挑战，尤其是检测方法的通用性低和适配难度高。因此，本文基于Windows系统的智能健康产品信息安全检测技术进行研究，提出适用于Windows系统和C/S架构软件的检测方法，并结合实际案例进行分析，从而为提升运行此类系统的智能健康产品信息安全水平提供实践指导与技术参考。

1　基于Windows系统的智能健康产品信息安全现状

在医疗行业，Windows系统因其具备设备通用性、开发便利性和用户熟悉度，被广泛应用于影像设备、检验设备等多种智能健康产品中。厂商选用Windows系统目的是降低医护人员学习成本，提升操作效率。然而，这类设备通常被部署在局域网内运行高度定制化的专用软件，其使用场景相对封闭单一，存在信息安全问题却不受重视[7]。

从供应链方面来看，在设备制造商的软件开发生命周期中，信息安全往往未被置于与功能同等重要的地位。对第三方组件、开源库的漏洞管理不充分，对底层固件安全性的验证不足，以及采购合同缺乏明确的安全基线要求均为设备埋下信息安全隐患。从设备生命周期来看，智能健康产品的使用寿命通常长达10～15年，远超普通IT设备更新周期。然而，随着微软终止对老旧Windows版本的支持，设备厂商却往往因缺乏动力或技术能力，无法为这些运行在旧版本系统上的设备提供持续的安全补丁或升级路径。此外，部分设备因固有软硬件性能的限制，系统难以部署第三方安全防护控件，设备的远程运维操作亦面临额外的风险[8]。

正是由于这些因素，使得运行Windows系统的智能健康产品仍存在诸多信息安全风险。使用STRIDE模型进行威胁建模[9]，可识别出近源攻击风险、数据安全风险及网络传输风险较为突出。

近源攻击风险主要体现在环境开放和人员意识薄弱2个方面。一方面，诊所的网络架构、现场物理环境等可能存在安全隐患，如无线局域网密码复杂度低、有线网络插口暴露在外、自助机配置不当等。攻击者可借此轻易接入内部网络，进而对智能健康产品发起攻击[10]。另一方面，人员信息安全意识薄弱也易引发风险，比如操作者违规使用移动存储介质、随意点击不明链接或下载未知附件等行为，都可能导致恶意软件在诊所内部网络传播，使其遭受感染和攻击。

数据安全风险主要体现在数据泄露与完整性破坏2个方面。一方面，智能健康产品软件漏洞、未经授权访问及人员不当操作等因素，均可能致使患者数据遭窃。这些数据若直接用于非医疗用途，则存在引发患者隐私泄露等严重后果[11-13]。另一方面，数据完整性和可用性也面临挑战，在数据全周期中，网络攻击、设备故障或人为干扰等因素，可能导致数据出错、丢失或被篡改，此外，部分医疗机构在数据存储管理上不规范，备份和加密措施不到位，一旦设备故障或遭受攻击，数据难以恢复。

网络传输风险主要体现在明文传输和网络配

置失效2个方面。一方面，智能健康产品在设计初期未对通信协议设计加密认证机制，会导致未加密的影像、检验报告等敏感数据在传输时易被截获、篡改或泄露，攻击者可通过网络嗅探窃取患者隐私信息[14-15]。另一方面，若存在使用默认密码、未设置或错误配置防火墙等网络配置不规范的问题，设备在网络传输过程中将直接面临被攻击的风险。这些安全风险可能引发连锁反应，导致整个网络系统被入侵，最终波及多个智能健康产品，干扰其正常运行。

2 相关法规与标准

近年来，智能健康产品信息安全愈发受到重视，各国为给智能健康产品信息安全提供规范指导与保障，陆续出台了多方面的相关法律法规与标准。2022年我国发布的《医疗器械网络安全注册审查指导原则（2022年修订版）》[16]从医疗器械网络安全注册审查的角度明确要求，注册申报资料、产品说明书、网络安全描述文档等诸多方面均应包含网络安全相关内容。而YY/T 1843—2022《医用电气设备网络安全基本要求》[17]则针对医用电气设备的网络安全特性规定，其应满足包括风险评估、安全功能、脆弱性处理等诸多基本要求，这些环节能够帮助开发厂商搭建智能健康产品网络安全的基础框架。

国际上，IEC 81001-5-1:2021 *Health software and health IT systems safety, effectiveness and security — Part 5-1: Security — Activities in the product life cycle*[18]聚焦于健康软件和IT系统的安全性问题。该标准强调在产品生命周期的设计、开发、维护等各个阶段，需开展相应的安全活动，以确保系统的安全性与可靠性。而UL 2900-2-1:2023 *Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems*[19]更关注医疗保健和健康系统中的网络连接产品。该标准提出对网络安全调查的具体要求，其涵盖漏洞评估、风险分析、安全测试等多个维度，为智能健康产品网络安全评估工作提供了全面且系统的指导。

以上法律法规与标准的制定与实施，为智能健康产品信息安全检测工作明确了方向。检测的基本框架、关键要素及具体要求让智能健康产品厂商、医疗机构及相关检测机构在开展信息安全检测与保障工作时有了明确参照。这对于提升智能健康产品信息安全水平、维护患者隐私与医疗数据安全有着重要意义，同时也为本文所研究的基于Windows系统的智能健康产品信息安全检测技术提供了坚实的法规依据与规范指导。

3 分析和评估方法

运行Windows系统的智能健康产品种类繁多，从功能到形态各有差异，但大体可归纳为两类。一类是分体式设备，这类设备以使用Windows系统的工作站作为操作终端，通过与智能健康产品主体相连，实现对设备的精准控制及诊断等关键操作，像常见的CBCT（锥形束投照计算机重组断层影像设备）就属于此类。另一类则是一体式设备，其特点是Windows上位机直接内嵌于智能健康产品之中，构成一个有机整体，如便携式超声设备，这种一体化设计便于在不同场景下灵活开展诊断工作。两类设备虽在架构上有所不同，但都配备了可操作的人机交互界面，医护人员可通过该界面便捷地输入指令、获取反馈信息，从而高效地运用智能健康产品开展各项诊断及治疗相关工作。针对运行Windows系统的智能健康产品具备可交互的特点，本文拟通过Kiosk模式绕过、系统漏洞攻击、USB接口攻击、内存读取、应用软件逆向、传输数据抓包等几个方式评估此类智能健康产品的信息安全。

3.1 Kiosk模式绕过

运行Windows系统的智能健康产品，为确保其专用性，通常会开启Kiosk模式，或经由注册表进行启动项配置，以此使设备在开机运行后能直接进

入应用软件登录界面，而非Windows桌面，这样的设置在一定程度上增强了系统安全性。然而，若配置不够完善，该安全功能则可能被绕过。一方面，可利用诸如粘滞键等快捷键，唤起系统弹窗，进而打开文件资源管理器，或者借助重启等方式进入安全模式，打开CMD命令进行配置变更。另一方面，智能健康产品中的GUI应用软件若提供了完整的Explorer（文件资源管理器）功能（见图1），同样可能导致绕过。比如在上传或下载功能处，尝试进行文件夹访问或新建文件等操作均可弹出Explorer导致Kiosk模式失效。若智能健康产品具备触屏功能，可在上下左右边框通过滑动的方式检查其滑动功能是否会致使Kiosk应用最小化，从而进入系统桌面。

此外，在设备启动环节可进行相关策略检查，如系统账户权限及BitLocker功能启动状态。（1）普通权限账户能够更精准地契合Kiosk模式的安全需求。相较于高权限账户，低权限账户通过最小化权限的管控，可有效缩小潜在的攻击面，降低因账户权限过高而引发的安全风险。（2）BitLocker功能的加密机制可全面阻止攻击者绕过正常认证流程或未经授权访问磁盘内容，在设备遭受物理盗窃或恶意拆卸硬盘的情况下也能确保数据的保密性与完整性。

3.2 系统漏洞攻击

对于运行Windows系统的智能健康产品，开发厂商普遍倾向选用长期服务频道（LTSC）、嵌入式版本（Windows IoT Enterprise）或仅提供扩展支持的稳定版本，这主要是为了保证软硬件的兼容性并减少开发成本。然而，这种对于系统稳定的追求并不等同于系统安全的保障。针对这类系统的风险，可通过先检查控制面板、运行命令行工具或进行网络扫描等方式，确认设备的操作系统版本、SKU、安装日期及关键安全补丁状态，然后识别厂商预装的软件清单，接着利用收集到的系统信息，在互联网上搜索相关的已知漏洞。信息源包括如美国国家漏洞数据库NVD之类的公共漏洞数据库、安全厂商发布的漏洞公告，以及Black Hat、HIPAA等安全会议的相关报告。最后根据这些漏洞信息进行POC（Proof of Concept，概念验证）测试或编写利用系统漏洞执行恶意操作获取系统权限或窃取数据的脚本进行攻击（见图2）。

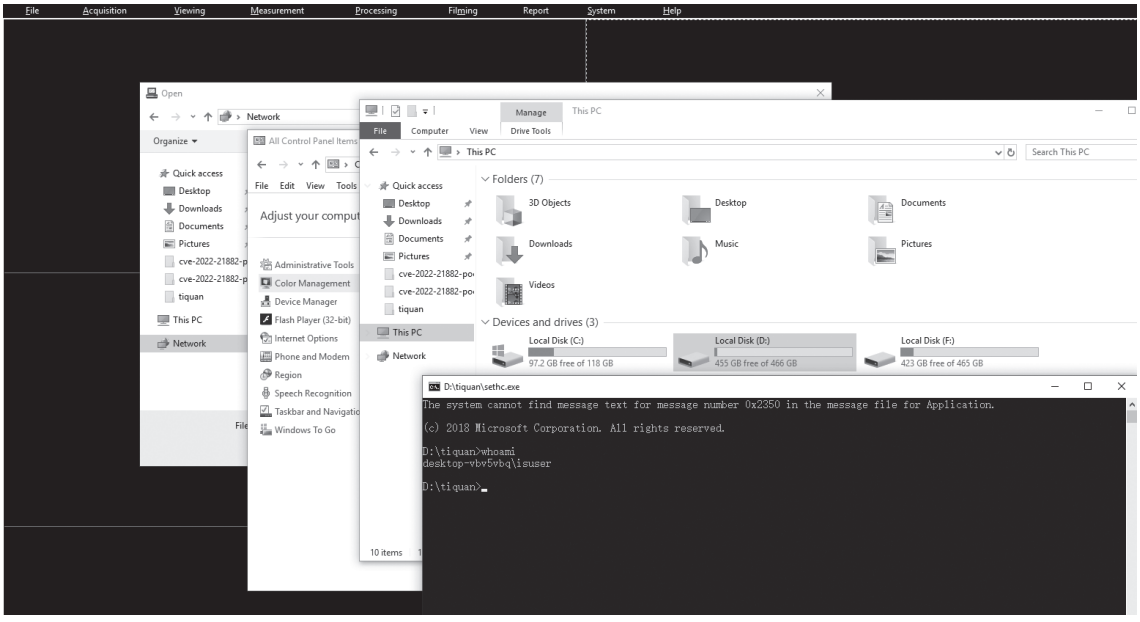

图1 在GUI应用软件中打开文件资源管理器

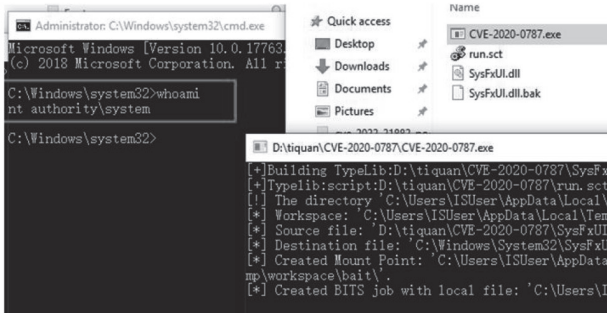

图2 使用CVE漏洞提升系统权限

3.3 USB接口攻击

在运行Windows系统的智能健康产品中，USB接口常用于打开从其他设备导出的医学影像或医疗数据。但因Windows系统默认启动自动加载功能，致使USB接口存在攻击风险。评估智能健康产品的USB接口防护措施时，可采用多种方法。（1）可尝试利用Bad USB等工具模拟鼠标或键盘，通过执行脚本模拟按键操作，查看设备是否能够抵御此类攻击，避免恶意软件植入、系统配置篡改、敏感数据窃取等操作（见图3）。据以色列研究团队统计，使用USB设备入侵用户计算机的方式多达29种[20]，基于此，可以检验智能健康产品是否具备完善的USB接口防护机制。（2）可检查智能健康产品是否通过设备管理器禁用了不必要的USB接口，或者是否使用端口锁定软件来限制USB设备的类型和使用权限。（3）还可检查是否对应用软件读取和执行移动存储设备中的文件类型实施了严格限制。该限制措施是为了保障USB接口的安全管理，防止恶意软件或未经授权的数据通过移动存储设备传播。

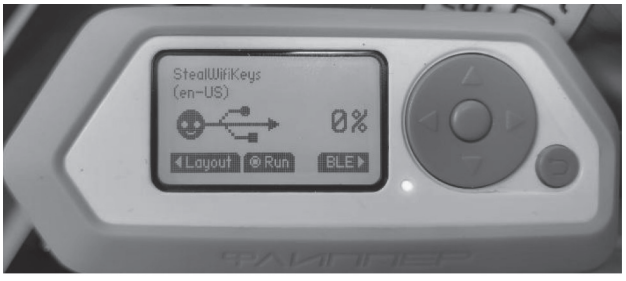

图3 使用Flipper Zero进行Bad USB攻击

3.4 内存读取

运行Windows系统的智能健康产品，通常配合C/S架构的智能健康应用软件一同使用。此类应用软件往往采用账号密码登录验证的方式来实施鉴权，这些用于鉴权的信息多存储于数据库之中。开发厂商在数据库的选择上，大多倾向于使用SQLite和Access之类的本地数据库。但无论是使用SQLite还是Access，其数据库文件通常直接存储在设备的本地磁盘上，应用软件在成功建立连接后，不是每次都会将连接字符串或关键的连接凭据重新输入，而是通常会将其临时缓存在进程堆内存或栈内存中。使用类似System Informer这类工具，能够读取内存信息，通过关键词搜索，可直接获取到连接数据库的密码（见图4）。一旦获取数据库文件及密码，即可直接访问数据库内容。若数据库采用明文存储数据，不仅可获取应用软件的鉴权信息，患者隐私信息和医疗数据也将面临严重泄露风险。

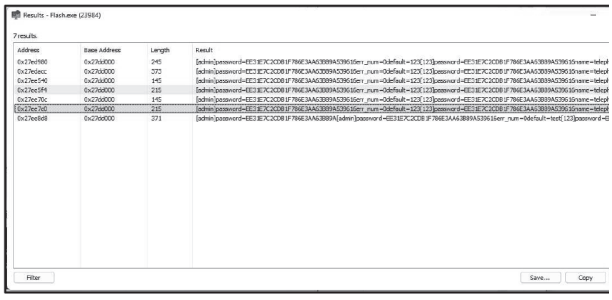

图4 通过System Informer读取登录密码

3.5 应用软件逆向

C/S架构的智能健康应用软件易遭受基于逆向分析的攻击。利用IDA Pro、Ghidra等专业工具对应用软件的可执行文件或安装包进行静态分析，可查找源代码中的硬编码明文敏感信息。例如，可分析软件的字符串区域、常量数据段、资源文件以及内嵌配置文件，直接检索数据库连接字符串、后台服务访问密钥、第三方集成API密钥等明文凭证或查看调试信息（见图5）。再者，可逆向分析软件加密算法逻辑，找出其加密和解密过程中的关键步骤和参数。例如，可通过DLL（Dynamic Link Library，动态链接库）导出关键加解密函数，利用该函数直接解密数据库中加密存储的敏感信息。此外，动态链接库注入和危险函数分析也是评估智能健康应用软件信息安全的有效方法，可用于检测智能健康应用软件是否存在潜在的安全漏洞和风险[21]。

```
41 64 6D 69 6E 31 32 33 00    aAdmin123 db 'Admin123',0
00 00 00                      align 4
61 64 6D 69 6E 00             aAdmin db 'admin',0
```

图5 使用IDA检索到账号密码

3.6 传输数据抓包

运行Windows系统的智能健康产品，常采用DICOM（Digital Imaging and Communications in Medicine，医学数字成像和通信）、HL7（Health Level Seven，卫生信息交换标准）等医疗通信协议传输医疗数据。理论上，其网络安全协议部分应采用基于证书授权（CA）的SSL（Secure Socket Layer，安全套接层）/TLS（Transport Layer Security，传输层安全）软加密技术保障数据传输安全。然而，实际应用中，因诊所智能健康产品检查设备数量众多、品牌杂乱、配置复杂，叠加终端网络性能受限，致使大部分诊所未能有效设置和使用传输加密功能[22]。因此，借助Wireshark等网络抓包工具，对智能健康产品在数据传输过程中的网络流量进行抓包操作，可重点分析数据包的载荷部分（见图6），未使用加密技术的数据包可查看到明文的医疗数据，如患者基本信息、检查结果、诊断报告等。此外，针对已启用TLS加密传输的智能健康产品，使用证书检测工具，检查其使用的数字证书是否由可信赖的证书授权机构颁发、是否在有效期内、是否与设备身份信息匹配等。若识别存在证书配置错误或使用无效证书的设备，可判定其在通信认证环节存在安全隐患。

4 结 论

近年来，智能健康产品的信息安全问题因医疗行业数字化转型而日益凸显，运行Windows系统的智能健康产品因其广泛应用于各行业成为信息安全关注的焦点。本文分析了包括近源攻击风险、数据安全风险和网络传输风险等基于Windows系统的智能健康产品在信息安全领域面临的挑战，并结合实际案例探讨了针对Windows系统和C/S架构软件的多种信息安全检测方法。然而，智能健康产品的信息安全形势随着人工智能、大数据和物联网等新兴技术在医疗领域的广泛应用将更加严峻，当前的检测工作仍存在一些亟待解决的问题，现有的检测技术在应对新型攻击手段和复杂网络环境时，仍存在一定的局限性，需要不断创新和完善。

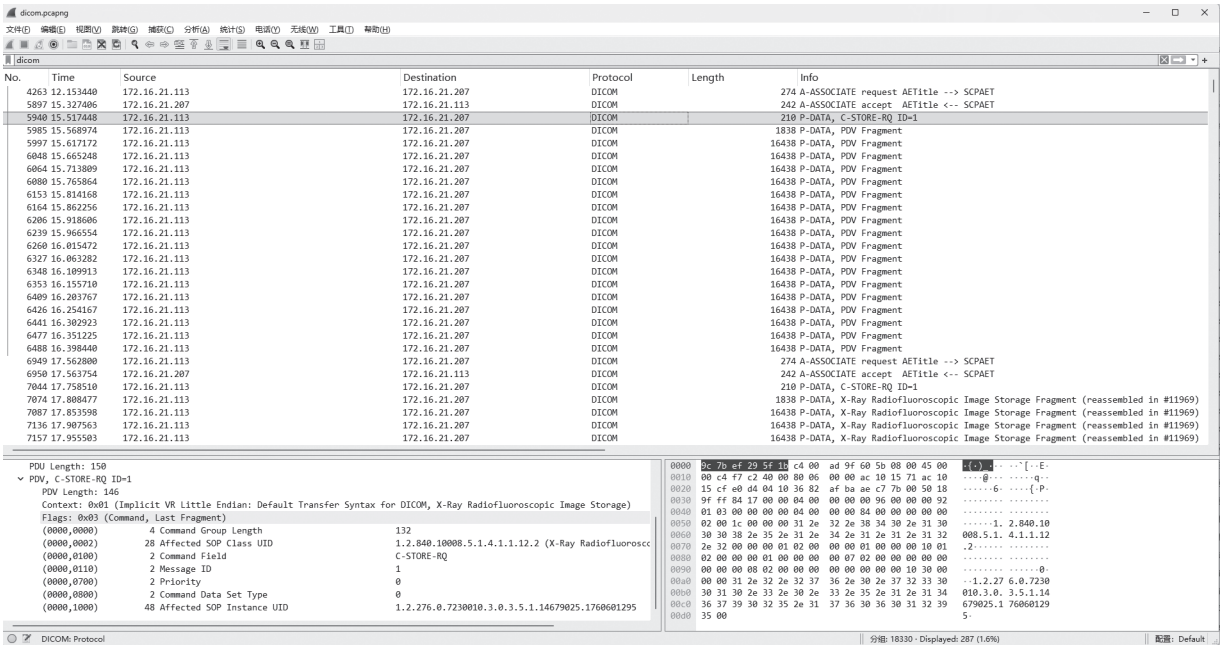

图6 使用Wireshark抓包查看DICOM数据

参考文献

[1] 田由辉.重大疫情背景下医疗数据网络安全防护研究[J].网络安全技术与应用,2020(6):140–142.

[2] 姜丛吾.移动医疗医院信息网络安全和对策探索[J].科技创新导报,2020,17(9):140.

[3] 王晨希,王权,李佳戈.医疗器械网络安全质量控制探讨[J].中国医疗设备,2021,36(9):23–27.

[4] 韩作为,李宏芳,赵韡.医疗设备全生命周期网络安全管理研究[J].中国数字医学,2023,18(9):6–9.

[5] 李文钰.浅谈医院信息系统的网络安全管理与维护[J].数字技术与应用,2023,41(4):222–224.

[6] 邱春旭,郑荣添,邹丹,等.渗透测试在医院信息系统网络安全管理方面的应用探讨[J].中国数字医学,2021,16(10):112–116.

[7] 郝鹏飞,李庆雨,柴蕊,等.医疗器械软件信息安全现状分析[J].中国医疗设备,2023,38(7):120–123.

[8] 闫维玮,邓越.医疗仪器设备网络安全风险评估与应对措施[J].中国新通信,2025,27(4):37–39.

[9] 姜宗伯,李澍,刘颖颖.基于Microsoft威胁建模工具的医疗健康场景下医疗器械网络安全问题分析方法[J].中国医疗设备,2023,38(12):113–118.

[10] 孟晓阳,杨巍,张楠,等.医院近源网络攻击风险分析及对策建议[J].医学信息学杂志,2024,45(9):87–90.

[11] 陈钿,蔡丹丹,李小江,等.医疗器械网络安全风险评估[J].中国医疗器械信息,2019,25(13):154–155.

[12] 郭进京,张雪,林鑫,等.国内患者隐私泄露情形及隐私保护现状分析[J].医学信息学杂志,2020,41(2):21–28.

[13] 林香,侯建勋,古锐鹏,等.浅谈医疗器械软件网络安全[J].网络安全技术与应用,2024(8):109–110.

[14] 田淼.医疗设备的网络安全挑战和应对[J].国际临床医学,2023,5(4):41–42.

[15] 刘奋达.探析医院信息网络安全管理及其维护措施[J].中国设备工程,2023(16):74–76.

[16] 国家药品监督管理局.医疗器械网络安全注册审查指导原则(2022年修订版)[EB/OL].(2022–03–10)[2025–06–10]. https://www.cncsdr.org/ggtz/ggzz/202203/t20220311_304187.html.

[17] 医用电气设备网络安全基本要求:YY/T 1843—2022[S].2022.

[18] Health software and health IT systems safety, effectiveness and security — Part 5–1: Security — Activities in the product life cycle: IEC 81001–5–1:2021[S].2021.

[19] Software Cybersecurity for Network–Connectable Products, Part 2–1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems: UL 2900–2–1:2023 [S].2023.

[20] Catalin Cimpan. Here's a List of 29 Different Types of USB Attack [EB/OL]. (2018–03–13)[2025–06–10]. https://www. bleepingcomputer.com/news/security/heres–a–list–of–29–different–types–of–usb–attacks/.

[21] 吴王震,李敏.医疗器械PC端软件网络安全测试方法研究[J].电子质量,2025(2):19–22.

[22] 蔡雨蒙,单红伟,王忠民.医学影像数据安全传输与管控系统的构建与应用[J].中国卫生信息管理杂志,2023,20(5):694–701.