

## 中华人民共和国公共安全行业标准

GA/T 1475—2018

---

### 法庭科学电子物证监控录像机 检验技术规范

Technical specifications for examination of electronic evidence in digital  
video record(DVR) in Forensics

2018-04-17 发布

2018-04-17 实施

---

中华人民共和国公安部 发布



## 前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

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

本标准由全国刑事技术标准化技术委员会电子物证检验分技术委员会(SAC/TC 179/SC 7)提出并归口。

本标准起草单位:北京市公安局刑事侦查总队刑事技术支队、公安部物证鉴定中心。

本标准起草人:贾永生、姚波、宋润、李荣荣、朱秀云、邢桂东、康艳荣。

# 法庭科学电子物证监控录像机 检验技术规范

## 1 范围

本标准规定了监控录像机电子物证检验的技术方法。  
本标准适用于法庭科学领域中对监控录像机进行电子物证的检验。

## 2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是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—2012 电子物证数据恢复检验规程

GB/T 29362—2012 电子物证数据搜索检验规程

## 3 术语和定义

下列术语和定义适用于本文件。

### 3.1

**监控录像机** digital video record; DVR

采用数字记录技术的视频录像设备。

### 3.2

**PC式监控录像机** DVR on PC

以计算机为硬件平台,配置视频采集卡及相应监控应用软件构成的监控录像机。

### 3.3

**嵌入式监控录像机** DVR with embedded system

非PC系统,以处理器、存储器、图形控制器、I/O端口等硬件为基础,以实时和多任务操作系统、可编程应用程序为软件平台,将内部的操作系统和应用程序写入到诸如FLASH、DISK ON CHIP或单片机等存储芯片上,组成一个完整的监控录像机。

### 3.4

**监控日志** monitoring log

监控录像机中对主机和外围设备进行重要操作及系统变动等信息的记录。

## 4 设备软件、硬件

### 4.1 硬件

存储介质复制设备、电子物证取证分析工作站、只读设备、仿真设备、专用存储介质、数码相机。

### 4.2 软件

存储介质取证分析软件、文件格式分析软件、视频播放软件、监控系统软件、数据恢复软件。

## 5 监控录像机检验

### 5.1 数据保全

5.1.1 对具有保全条件的检材,使用存储介质复制设备复制被检录像机内置硬盘、存储卡等存储介质(以下简称存储介质),制成存储介质镜像并进行哈希校验,镜像应有唯一性编号。

5.1.2 应使用存储介质镜像(在源存储介质不具有保全条件时可使用源存储介质检验)并在只读状态下进行检验。

### 5.2 PC式监控录像机检验

#### 5.2.1 基础检验

5.2.1.1 使用电子物证取证分析软件对存储介质镜像的数据进行分析。

5.2.1.2 分析确定监控录像机监控、录制、播放使用的软件,并提取。提取的软件在电子物证取证分析计算机上不能正常运行时,需通过生产厂商等渠道获取专用软件或其他兼容软件,以确保能够读取视频上叠加的通道、时间等信息。

5.2.1.3 分析确定监控录像机录制视频的格式。

5.2.1.4 分析确定视频中嵌入时间码的方式。

5.2.1.5 分析确定视频文件的命名规则。

5.2.1.6 查看监控录像机的系统时间与录像机所在地的标准时间,并记录。

#### 5.2.2 监控日志检验

5.2.2.1 使用存储介质检验分析软件在存储介质镜像内搜索监控日志文件,并提取:

- a) 使用文件格式分析软件解析、查看日志文件,并导出为常用格式的文档文件;
- b) 如果文件解析软件不支持对日志文件的解析,则尝试运行监控录像机内置的监控软件查看日志文件,并导出为常用格式的文档文件。

5.2.2.2 如果通过 5.2.2.1 步骤不能实现对日志文件的解析,则按以下步骤进行开机检验:

- a) 将存储介质镜像通过仿真设备接入监控录像机的数据接口;
- b) 启动计算机进入操作系统;
- c) 查找系统内的监控软件并运行;
- d) 使用监控软件的日志查看功能查看监控日志并导出为常用格式的文档文件;
- e) 如果通过以上步骤不能导出监控日志,则使用屏幕截图或拍照的方法进行提取。

#### 5.2.3 视频数据检验

5.2.3.1 将存储介质镜像接入电子物证取证分析工作站。

5.2.3.2 使用存储介质检验分析软件在存储介质镜像内按照 5.2.1.3 确定的视频格式搜索监控视频文件。

5.2.3.3 使用被检监控录像机专用播放软件或其他兼容视频播放软件进行视频播放、查看。

5.2.3.4 提取相关视频文件。

5.2.3.5 如果以上步骤未检出相关视频,依据 GB/T 29360—2012、GB/T 29362—2012 对存储介质镜像进行数据检验,再按照 5.2.3.1~5.2.3.4 步骤操作。

### 5.3 嵌入式监控录像机检验

#### 5.3.1 监控日志检验

##### 5.3.1.1 通过主板存储监控日志的监控录像机的日志检验

5.3.1.1.1 确保录像机的内置存储介质已断开与主机的连接。

5.3.1.1.2 启动监控录像机进入操作界面。

5.3.1.1.3 如通过上述步骤不能启动监控录像机,则通过仿真设备将存储介质镜像接入监控录像机,再启动进入录像机操作界面。

5.3.1.1.4 查看监控录像机的系统时间与录像机所在地的标准时间,并记录。

5.3.1.1.5 查找日志相关选项,查看并分析监控日志。

5.3.1.1.6 监控录像机具有日志备份功能的,将日志备份并存储到具有唯一性编号的专用存储介质中。

5.3.1.1.7 监控录像机不具有日志备份功能的,使用屏幕拍照的方法提取监控日志。

##### 5.3.1.2 通过存储介质存储监控日志的监控录像机的日志检验

5.3.1.2.1 使用存储介质取证分析软件分析存储介质镜像数据,搜索监控日志文件并提取。

5.3.1.2.2 使用文件解析软件解析、查看日志文件,并导出为常用格式的文档文件。

5.3.1.2.3 如以上步骤不能搜索到监控日志文件,则按以下步骤进行开机检验。

5.3.1.2.4 将存储介质镜像通过仿真设备接入监控录像机。

5.3.1.2.5 启动监控录像机进入操作界面。

5.3.1.2.6 查找日志相关选项,查看并分析监控日志。

5.3.1.2.7 监控录像机具有日志备份功能的,将日志备份并存储到具有唯一性编号的专用存储介质中。

5.3.1.2.8 监控录像机无法导出日志的,使用屏幕拍照的方法提取监控日志。

#### 5.3.2 视频数据检验

##### 5.3.2.1 通过监控录像机备份功能导出监控视频

5.3.2.1.1 将存储介质镜像通过仿真设备接入监控录像机。

5.3.2.1.2 启动监控录像机进入操作界面。

5.3.2.1.3 查看监控录像机系统时间与录像机所在地的标准时间,并记录。

5.3.2.1.4 使用监控录像机的视频播放功能搜索视频进行播放并查找相关视频内容。

5.3.2.1.5 使用监控录像机的视频备份功能将相关视频以文件方式备份至具有唯一性编号的专用存储介质。

##### 5.3.2.2 通过底层数据恢复的方法提取监控视频

5.3.2.2.1 在监控录像机不具备视频备份功能或视频被删除、存储介质被格式化、系统被初始化等情况下,需要按以下步骤对存储介质进行底层数据恢复。

5.3.2.2.2 将存储介质镜像以只读方式接入电子物证取证分析工作站。

5.3.2.2.3 使用数据恢复软件对存储介质镜像数据进行搜索。

5.3.2.2.4 分析、查找每段视频数据存储的起始位置和结束位置。

5.3.2.2.5 以十六进制复制 5.3.2.2.4 中查找的数据,并按被检监控录像机使用的视频编码格式存储为相应的视频文件。导出的视频文件应存储在具有唯一性编号的专用存储介质中。

GA/T 1475—2018

5.3.2.2.6 使用监控录像机专用播放软件或其他兼容视频播放软件播放导出的视频文件并进行内容筛查。

## 6 检验结果保存

将检出数据采用封盘刻录方式刻录在不可擦写的空白光盘上或者保存在专用存储介质中,并计算检出数据的哈希值。

## 7 检验结果表述

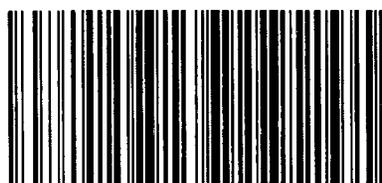
检验结果表述应符合以下规定:

- a) 检验结果分为检出、未检出、不具备检验条件 3 种;
- b) 检验结果应根据检验要求对检验对象、检验范围、检验所得进行客观、概括、有针对性的描述;
- c) 结果表述应包含检材编号、检出情况、检出数据文件或保存检出数据介质哈希值、保存检出数据介质编号等必要信息。

## 8 附则

8.1 开机检验时应断开存储介质的连接,如需带存储介质启动,在条件允许的情况下应通过仿真设备连接。

8.2 导出的数据及拍照提取的内容均应使用专用存储介质存储。



GA/T 1475-2018

版权专有 侵权必究

\*

书号:155066·2-44715

定价: 14.00 元