CDF BOOT CAMP
电子数据取证技术训练营

实验

取证工作站/证据固定

目录

3.1 实验内容.....1
3.2 实验目的.....1
3.3 实验环境.....1
3.4 实验原理和方法.....1
3.4.1 证据固定.....2
3.4.2 磁盘镜像.....2
3.4.3 物理磁盘和逻辑磁盘.....7
3.4.4 磁盘镜像设备和软件.....8
3.5 实验步骤.....11
3.5.1 实验 1：创建 VHD 虚拟磁盘.....11
3.5.2 实验 2：利用 Winhex/X-Ways Forensics 获取磁盘的物理镜像.....14
3.5.3 实验 3：第三章课后习题.....18
3.5.4 获取 Bitlocker 加密磁盘镜像.....21
3.5.6 使用 DD 命令获取镜像解密的 Bitlocker 磁盘镜像.....24

3 证据固定

3.1 实验内容

证据固定，是取证环节的第一步，是在熟练的使用适用工具的前提下，对不同状态、不同类型的计算机和存储介质进行磁盘镜像，做到流程规范、步骤清晰、证据合规。本实验主要针对电子数据取证中较为常见的几种磁盘镜像进行学习，重点练习制作磁盘镜像的方法和工具，并利用工具，进行证据的获取、哈希验证、格式转换、镜像挂载等。

本章实验主要内容：

任务 1：创建 VHD 虚拟磁盘

任务 2：学习使用 FTK 创建物理磁盘镜像

任务 3：计算并校验磁盘和镜像文件哈希值

3.2 实验目的

学习磁盘镜像的格式、类型。掌握有关磁盘镜像的工具。通过完成实验内容，要求学生可以自行创建虚拟磁盘、挂载磁盘镜像、创建磁盘镜像。对各种磁盘镜像文件格式、Windows 系统下的磁盘镜像工具，不同状态下的证据固定方法全面的了解。对各类磁盘镜像文件的的异同进行梳理分析、并在实际操作中归纳各类磁盘镜像的特点及规律。

1.学习 Windows 下 VHD 虚拟磁盘的制作方法

2.学习 FTK Imager，创建磁盘镜像

3.学习猎痕镜像挂载工具，挂载特殊格式镜像文件

3.3 实验环境

1.FTK Imager、猎痕镜像挂载软件

2.案例文件：A01-FAT-Disk.001

3.4 实验原理和方法

3.4.1 证据固定

在电子数据取证中，经常会提到证据固定、磁盘镜像、证据文件等名词。真实案件中，执法人员可能需要对几十台计算机、服务器、磁盘阵列、大量的移动存储介质、视频录像机硬盘进行封存和证据固定。企业内部调查案件中，经常对嫌疑人的硬盘、服务器硬盘、内存、日志进行取证。有效力的电子数据，是进行案件调查、数据分析、司法鉴定的前提。然而，有些情况下，证据可能因为各种原因随时灭失或发生变化，从而影响证据的效力，阻碍案件的进展。这些情况下，符合资质的人员需要采用适用的工具，遵循一定的流程和标准，将不同状态下的电子数据及时获取并安全保存。

证据固定，即将嫌疑计算机或存储介质的数据进行获取的过程。证据固定必须符合严格的操作规范，并且需要由具有专业资质的人员使用专业的数据获取工具进行。证据文件格式应符合司法接受的标准。

3.4.2 磁盘镜像

为了保证电子数据的原始性，取证实践中为避免操作人员对原始证据进行直接操作而造成原始证据的数据改变，办案人员要对原始数据进行磁盘镜像，分析过程中对磁盘镜像进行操作。磁盘镜像也是一种保护电子数据真实性、唯一性的有效方法。在国内外取证规则和指南中，制作磁盘镜像，是进行电子数据取证的必不可少的一个环节。

磁盘镜像，是指对原始数据逐比特位进行复制，从而产生与原始数据完全一致的镜像数据。除了原始的磁盘数据之外，可增加不同类型的元数据信息将镜像文件予以增强，例如增加错误检测、数据哈希、不同性能的压缩算法等，这样就演化出一些不同的镜像格式。目前比较典型的有 DD、E01、Smart 格式等。

对于磁盘镜像，我们可以理解为：

1. 镜像是原始电子数据的副本，逐比特位的保存有原始数据；
2. 镜像可以由一个完整文件构成，也可以由一系列分段文件组成；
3. 镜像内容与原始数据内容一致，可以看做原始数据，并作为证据使用和保存。

取证中几个易混淆的术语：

镜像（Image）：将磁盘所有数据同样写入到一个文件。删除数据可恢复。

克隆（Clone）：将磁盘所有数据同样写入到另一个磁盘。删除数据可恢复。

备份（Backup）：将磁盘逻辑文件写入到一个文件。删除数据不可恢复。

复制（Copy）：将磁盘逻辑文件或文件内容转移到另一个位置。删除数据不可恢复。

磁盘镜像格式主要有原始格式、专有格式和虚拟机磁盘。

常用的证据文件格式有 DD 和 E01 镜像格式（也称做 Expert Witness 证据文件格式）。目前，国内法院并

未对证据文件格式，如果证据文件需进行国际诉讼，建议使用国际通用的取证工具，并选择 E01 镜像格式。为了保证证据文件真实有效，获取证据同时需要利用特定的哈希算法（例如 MD5 算法）计算并验证证据文件的哈希值。虽然 MD5 算法被我国科研人员证实为存在漏洞，但至今各国法庭仍然普遍接受 MD5 验证值，因此调查人员依然可以采用 MD5 算法对证据文件进行计算并验证。实践中，需要妥善记录、保存原始的哈希值、校验值，以备法庭指派的第三方机构重新验证，确保证据文件的有效性。

1.DD 镜像格式

原始格式，最早起源于 DD 命令，因此被简称为 DD 镜像格式。是对原始磁盘或卷进行的位对位的复制，原始镜像中的数据不会有任何增加或减少。原始格式镜像文件中，不包含任何描述镜像文件的元数据信息。需要记录的元数据，如操作时间、磁盘信息、哈希值等，会保存在一个单独的文本文件中。

DD 镜像格式的特点：

第一，兼容性好。DD 镜像格式是被最广泛使用的一种镜像格式，所有磁盘镜像和分析工具都支持 DD 镜像格式。

第二，占用空间大。镜像文件与原始证据磁盘容量完全一致，未被压缩，因此需要较大的存储空间。即便原始证据磁盘仅有很少的数据，也一样需要同样的磁盘容量。例如一个磁盘容量为 1TB，存储数据只有 10GB，磁盘镜像文件仍需要 1TB。

第三，数据处理效率高。想解决 DD 镜像文件占用空间大的问题，最简单方法就是利用数据压缩技术。但是无论使用哪种数据压缩方法，在分析时必然要经过一个解压缩的过程，这就造成了分析效率低下。DD 镜像采用非压缩格式，因此数据处理效率是在所有镜像格式中最高的。

第四，元数据需要单独保存。DD 镜像是对嫌疑硬盘进行位对位的复制方法，生成的镜像文件中没有保存额外信息的空间。因此，例如硬盘序列号、调查员姓名、创建镜像的时间和地点等信息必须保存在镜像文件之外的单独文件中。由于这些信息没有被保存在镜像文件内部，就有可能造成一些不便。例如，如果描述文件容易丢失，也容易和其他镜像文件混淆。

2.EnCase 镜像格式

E01 是法证分析软件 EnCase 的一个证据文件格式，较好地解决了 DD 镜像带来的一些问题。EnCase 以一系列特有的压缩片段格式保存证据文件。每一个片段都可以在需要时被单独地调用并解压缩，因此可以实现随机访问镜像中的数据。

EX01，是 Encase 7.0 版本之后出现的新的镜像格式，仍然包含压缩和加密选项。

镜像文件分段：镜像文件可以是一个单独存在的文件，也可以是由连续的固定大小的分段文件构成。分段

大小可以设定任意数值，但通常默认值有 640MB、1GB、2GB、4GB 等大小。任何一个镜像分段文件受损或缺失，都会造成完整镜像文件无法成功打开。

EnCase 证据文件中包含有三个组成部分：文件头、校验值和数据块。这三部分组成了对于一个原始证据的描述，并可用于将证据文件重新恢复至硬盘。但 DD 镜像文件不包含文件头和校验值，相关数据信息可以配合 TXT 文本形式文件进行描述。

EnCase 在生成 E01 格式证据文件时，会要求用户输入与调查案件相关的信息，如调查人员、地点、机构、备注等元数据。这些元数据将随证据数据信息一同存入 E01 文件中。文件的每个字节都经过 32 位的 CRC 校验，这就使得证据被篡改的可能性几乎为 0。在默认情况下，分析软件自动以每 64 扇区的数据块进行校验，这种方式兼顾了速度和完整性两方面的考虑。

E01 格式最大的问题就是兼容性问题。由于 EnCase 格式是非公开的、具有知识产权的商业软件镜像格式，因此没有人明确地知道这种格式的全部细节。尽管一些开发人员反编译了 E01 格式并提供了具有一定兼容性的支持，而且很多软件也能够打开 E01 文件或者可以创建 E01 文件，但同时很多公司都声称，不对因 E01 兼容性问题造成的数据问题负责。因此用户需要注意的是：除该格式的原始研发公司之外，其他公司所掌握的 E01 格式均不全面。

3. AFF 镜像格式

针对 E01 和 DD 镜像文件的不足， AFFLIB 公司于 2006 年推出了开源的证据文件格式 AFF 格式（Advanced Forensics Format ），这种格式是公开而且可扩展的。目前 Autopsy 和 The Sleuth Kit 都支持此格式。

相较于 EnCase 证据文件格式，AFF 镜像也以压缩片段的方式保存磁盘镜像，镜像文件经过压缩后容量明显减小。和 EnCase 镜像不同的是，AFF 镜像既可以将元数据保存在镜像文件内部，也同时允许元数据被单独保存在一个文件中。尽管 AFF 格式是为了解决同时应对成百上千个磁盘镜像任务而设计的，但同样也只适用于一至两个硬盘的小型案件。一旦发生磁盘镜像文件破损的情况， AFF 镜像的内部连续性算法也能够保证尽可能多地将破损的磁盘镜像修复。

AFF 分段镜像可以被开源工具 zlib 进行压缩，也可以保持未压缩状态。AFF 镜像压缩格式可以节省空间，但是创建时间较长，而且分析处理的速度较慢。具体采用压缩与否，可依据实际情况来决定，且未压缩的 AFF 镜像文件可以很容易地再次压缩。

AFF 格式不涉及版权问题，该格式是开源的，可以被任何开源工具或商业软件使用。现在这种格式已经被越来越多的厂商所采纳，并将逐渐成为了一种标准的镜像格式。

4. AFF4 镜像格式

AFF4，高级取证文件格式，基于 AFF 格式发展而来，是一种开放源镜像格式，用于存储数字证据。

5. Smart 镜像格式

ASRData 公司开发的 Smart Linux 专有镜像格式。

6. ProDiscover 镜像格式

美国取证软件 ProDiscover Forensics 专有镜像格式。

7. 虚拟磁盘文件

虚拟机在各种场景中被广泛的使用。很多案件、练习题、考核中，经常会出现在一个磁盘中存放其他的虚拟机硬盘文件，内置了不同的操作系统、文件系统、应用程序。

主流虚拟机软件有 VMware、VirtualBox、Parallel Desktop 等。当用户创建虚拟机时，虚拟机软件会为该虚拟机创建一组文件。这些虚拟机文件存储在虚拟机目录或工作目录中。

虚拟磁盘文件，用于存储虚拟机硬盘驱动器的内容。常见的虚拟机磁盘文件类型有 VMDK、VHD、VDI、DSK 等。

一个虚拟磁盘由一个或多个虚拟磁盘文件构成。 如果创建虚拟磁盘时，用户指定位“固定大小”，例如设置 100GB 磁盘空间，这个文件一开始就会是最大容量 100GB，之后也不会再增长。如果用户指定为“动态分配”，则虚拟硬盘是逐渐占用物理硬盘空间，随用户数据量增加不断扩充容量，直至达到分配的大小。有些虚拟机软件可以设置虚拟磁盘分段，例如用户设定将虚拟磁盘设定为 2 GB 大小的分段文件，文件数量取决于虚拟磁盘的大小。随着数据被添加到虚拟磁盘，每个文件最大可以扩至 2 GB。

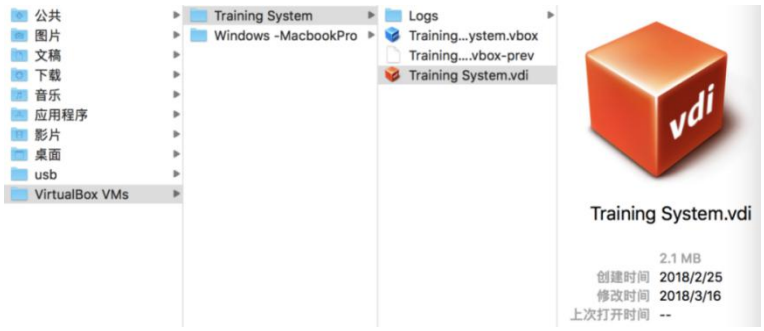

图 3-4-1 VirtualBox 虚拟机硬盘文件

表 3-1 主流虚拟机镜像格式

扩展名	软件	描述
VHD VHDX	Windows Virtual PC	VHD 是 Virtual Hard Disk 的简称。可以由部分版本的 Windows、Virtual PC、Virtual Box 等直接创建。

VDI	Virtual Box	Virtual Disk Images，Virtual Box 软件的虚拟磁盘文件
VMDK	VMware	VMware 软件的虚拟磁盘文件。 如果设定的磁盘大小可以增加，文件名的文件编号部分将包含一个 s，例如 Windows 7-s001.vmdk。 如果在创建磁盘时分配了全部磁盘空间，文件名中将包含一个 f，例如 Windows 7-f001.vmdk。
HDD	Parallels Desktop	Parallels Desktop 的虚拟磁盘

表 3-2 VMware 相关文件描述

扩展名	描述
.vmdk	VMware 软件的虚拟磁盘文件。虚拟机取证中，通常主要关注.log、.vmdk、.vmem 三个文件，里面包含虚拟机的大部分资料信息。
.vmem	虚拟机-内存文件。虚拟内存文件，同本地内存文件 pagefile.sys（分页文件），包含了操作系统的内核数据结构、进程、线程、堆中的数据，以及用户的其他如用户输入的密码、聊天信息等敏感信息；正常虚拟机中的系统关机后，vmem 文件就会消失；但虚拟机的系统在挂起状态时，该文件会保留在本地。
.vmsd	用于存储元数据和虚拟机快照文件的描述信息，信息包括 UID 编号、快照文件名、快照注释、执行快照的磁盘文件和快照总数等。初始大小为 0 字节，随着快照数的增加而持续增大。把.vmsn 和.vmdk 记录一起。
.vmsn	虚拟机-建立快照时自动创建的文件，配合.vmsd 文件使用。【虚拟机-快照】中[虚拟机名-Snapshot 快照名.vmem]和[虚拟机名-Snapshot 快照名.vmsn]文件是成对出现的。无快照则该文件没有。
.vmss	虚拟机-已挂起状态时的信息文件（虚拟机挂起状态才有！）【虚拟机-挂起状态】中[虚拟机名-xxx.vmem]和[虚拟机名-xxx.vmss]文件是成对出现的。
.vmx	虚拟机-硬件配置文件
.vmxf	虚拟机-附加配置文件
.nvram	储存虚拟机 BIOS 状态信息
.log	虚拟机-调试运行情况的日志记录；如文件创建、USB 接入、虚拟机运行的情况、操作系统

	基本信息、用户行为时间等。vmware-0.log、vmware-1.log 等用来记录 vmware 工作日志。
.lck	动态文件保存目录。该目录是虚拟机系统在开机时自动创建的以.lck 结尾的目录，作用是用于锁定 vmx 的文件夹，在虚拟机关机后会自动删除。也用于在虚拟机异常退出时为了保护虚拟系统的磁盘文件数据而保留的.lck 结尾的文件及文件夹。在开启虚拟机系统时，如出现“虚拟机正在被使用，获取所有权的报错”，可将其删除，一般就可正常开启虚拟机。

图 VMware 相关文件

3.4.3 物理磁盘和逻辑磁盘

物理磁盘：包含整个磁盘空间。针对整个物理磁盘进行的镜像称为物理镜像。

逻辑磁盘：磁盘经过分区后，操作系统会对分区分配盘符。这样每一个具有盘符的分区都是一个逻辑分区，也被称为逻辑磁盘。针对特定分区进行的镜像称为逻辑镜像。例如只有 C 盘或 D 盘，也可以针对某个目录和文件制作镜像，同样为逻辑镜像。

图 3-4-2 物理磁盘和分区

按照取证原则，证据固定，应该对完整的磁盘创建磁盘镜像，这样可以包含所有的数据信息。大多数取证工具，都支持对物理磁盘或逻辑磁盘的数据获取功能。情况下，取证人员只需要利用工具选择物理磁盘即可。

某些情况下，物理磁盘有部分磁道损坏，无法完整获取磁盘镜像。但是某些分区是完整的，没有任何损坏。这时候，可以进行逻辑获取，对其中的比较完整的分区进行磁盘镜像。此外，有些国际诉讼中，案件要求不得对与案件无关的数据进行获取，只能提取涉案文件，例如电子邮件。此时，取证人员可以只针对电子邮件目录进行证据固定。

3.4.4 磁盘镜像设备和软件

目前各种取证工具基本具有磁盘镜像功能。

1. Falcon NEO

美国 Logicube 公司十几年来一致致力于研制用于司法实践的电子数据硬件获取产品是硬盘复制和数字取证行业的领导者。旗下的 Forensic Falcon 目前被认为是领先的高科技司法取证解决方案之一，其各项功能都在行业内领先，制作镜像的速度高达 50GB/分。Forensic Falcon 的多任务功能，还可允许用户同时镜像、擦除、哈希，大大提高了效率，缩短了获取证据的时间，并且独有的并行镜像功能能够将同一个源盘以不同的格式制作镜像到不同的目标盘。Forensic Falcon NEO 的套件支持 SAS/SATA/USB/Firewire 接口，通过转接头可支持 IDE、eSATA、mSATA、 microSATA 和闪存盘(CF 卡、SD 卡等)。

图 3-4-3 Logicube 公司的 Falcon 和 Falcon NEO

2. Tableau TX1

美国 Guidance Software 公司是全球计算机调查与取证卓越的先驱者领航者，也是全球最大的取证软件提供商，客户遍布全世界。该公司一直致力于为取证人员提供计算机犯罪取证的全面解决方案，Tableau TD3 是其最新一代的 TD 系列的硬盘复制机，它具有高性能、稳定性好、便于使用等特点。

Tableau TD3 是第三代 TD 系列硬盘复制机。用户如果要复制 SATA、USB、Firewire 等接口的硬盘，直接连接到 TD3 上即可。如果想要对 SAS 和 IDE 硬盘做镜像，通过 TDPX 适配器连接 TD3 即可。TD3 具有一个 Gigabit Ethernet 连接，能用来镜像或者上传镜像证据到 iSCSI 或 CIFS 网络文件分享中。当用户需要远程预览和收集数据时，TD3 可以通过设置 IP 地址，让远程 PC 通过互联网访问 TD3。

图 3-4-4 TD3 硬盘复制机

Tableau 较新型号的硬盘复制机是 TX1，可配备扩展接口支持 IDE 硬盘、输入至 4 个 SATA/SAS 接口。支持的镜像格式包括 DD、DMG、E01、ex01，支持的文件系统有 exFAT、NTFS、EXT4、FAT32、HFS+。外观和支持的接口如下图所示。

图 3-4-5 TX1 硬盘复制机

设备操作界面简介，快速进行镜像、校验、哈希和浏览。如下图，所示：

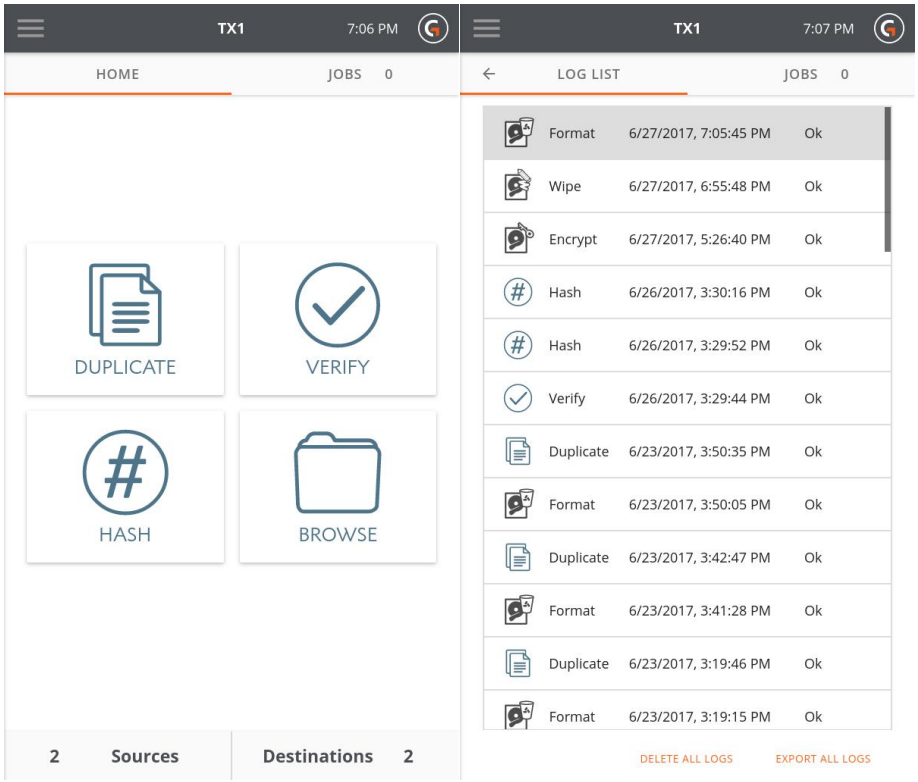

图 3-4-6　TX1 硬盘复制机界面

3. Solo4 G5

美国 ICS 公司是硬盘复制行业的先驱，是全世界第一家引入硬盘复制技术的企业。公司的产品从 Solo 2 开始即在取证行业带来了变革，后续推出了 Solo 3、Solo4 和 Solo4 G3。目前 Solo 5 是最新一代的硬盘复制机。Solo4 的复制速度为 6GB/分钟，Solo4 G3 的复制速度可达 27GB/分钟的速度（基于 SSD 测试）。Solo 5 的速度达到 69GB 的速度。

Solo4 G3 与 Solo4 的大部分功能基本相同：支持同时对两块 IDE、SATA、SCSI、SAS 硬盘以及 USB 移动存储设备进行取证。其内嵌 RAID 功能模块，支持对 RAID 硬盘进行取证，同时支持免拆机取证功能，直接通过 USB 或网络接口获取嫌疑数据。Solo4 G3 还是一个能够对 Android、iOS 手机进行快速取证的专业手机取证设备。由于 Solo4 G3 价格昂贵，目前国内机构选择较多的还是 Solo4。

图 3-4-7　Solo 5 硬盘复制机

Solo 5 包括 4 个 SAS/SATA，6 个 USB 3.0，2 个 eSATA，2 个 Firewire 800，1 个 Firewire 400，2 个

PCIE 扩展口。其中 2 个 SATA/SAS 和 2 个 USB 3.0 为只读接口。

4.FTK Imager

由于对存储介质进行镜像是电子数据取证中必不可缺的步骤，因此很多主流取证软件厂商将镜像软件独立成产品，大多数都是免费产品，起到宣传综合取证软件的作用。FTK Imager 是 AccessData 公司出品的一款免费镜像制作软件，具有数据预览、证据镜像制作、加载证据镜像等功能，能够支持目前几乎主流的文件系统，能够加载和生成包括 DD、E01、Smart、AFF 格式的证据镜像，使用起来十分方便。

5.Belkasoft Acquisition Tool

简称 BAT，俄罗斯 Belkasoft 公司免费工具，可以帮助调查员完成取证过程中最重要的证据获取环节。支持硬盘镜像、内存获取、手机数据获取、云数据获取。

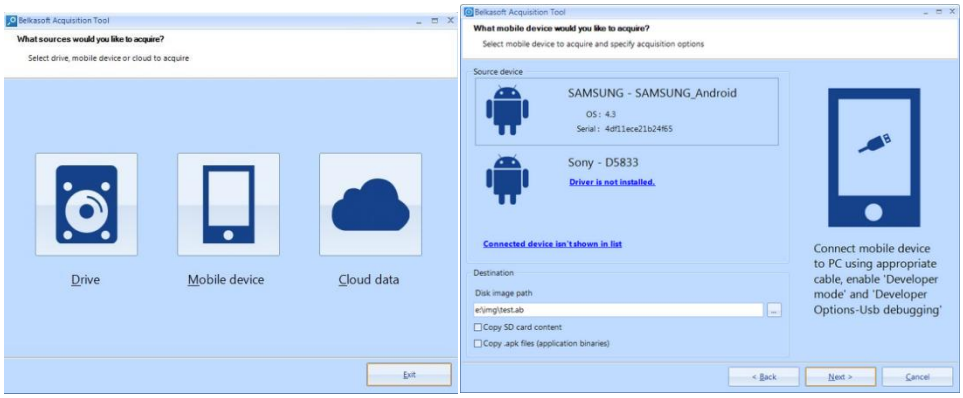

图 3-4-8 BAT 界面

3.5 实验步骤

3.5.1 实验 1：创建 VHD 虚拟磁盘

场景：对一台笔记本计算机硬盘和 U 盘进行证据固定。

工具准备：取证教学环境、磁盘管理工具

实验目标：创建一个用于练习证据固定使用的虚拟磁盘

1.创建一个 1GB VHD 虚拟磁盘

调用 Windows 磁盘管理，通过操作菜单，选择创建 VHD。

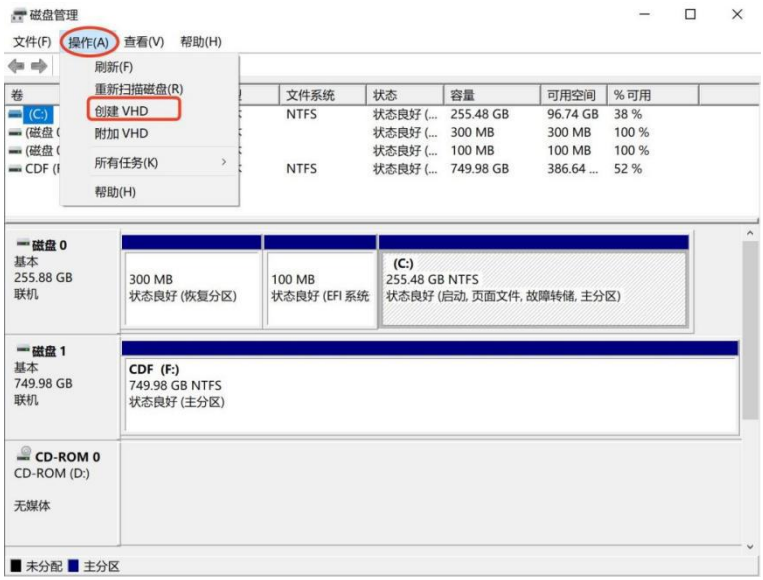

图 3-5-1-1 创建 VHD

2. 选择保存位置，VHD 虚拟磁盘容量设为 1GB。

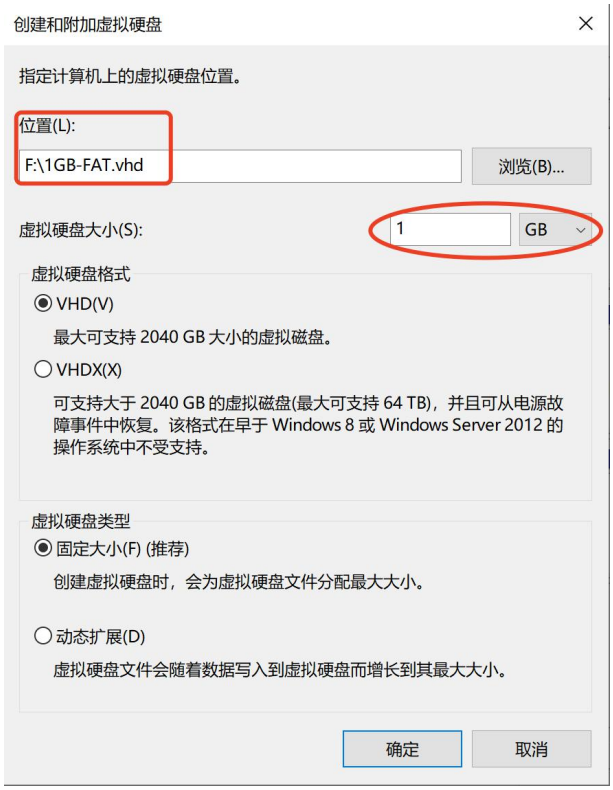

图 3-5-1-2 设置虚拟磁盘文件名、路径和大小

3. 选择 VHD 虚拟磁盘容量，鼠标右键点击，选择“初始化磁盘”

图 3-5-1-3 初始化虚拟磁盘，选择 MBR 分区模式

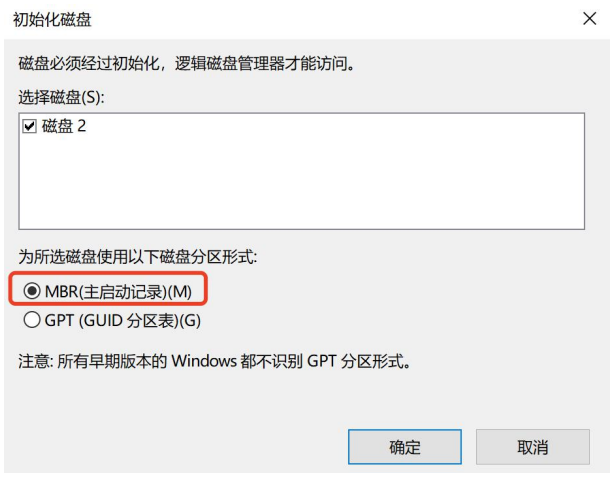

图 3-5-1-4 选择 MBR 分区模式

图 3-5-1-5 初始化成功，显示联机

提示：此时可以利用 Winhex 加载新创建的 VHD 磁盘，查看 MBR 标志：55 AA。理解 MBR 的概念。

4. 选择 1GB VHD 虚拟磁盘，鼠标右键点击，选择“新建简单卷”

图 3-5-1-6 右键，选择“新建简单卷”

5. “新建简单卷”向导，分为 2 个分区。第一个卷大小为 512MB。文件系统设为 FAT32。剩余空间都留给第二个卷，约为 509MB，文件系统设为 FAT32。

图 3-5-1-7 右键，设置、调整分区大小

图 3-5-1-8 格式化新建卷

6. 点击“此电脑”——“设备和驱动器”中，查看创建的 VHD 虚拟磁盘。同时至保存虚拟磁盘文件的位置，查看刚刚创建的 1GB-FAT.vhd 虚拟硬盘文件。

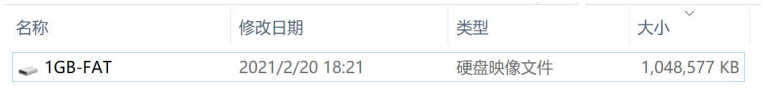

图 3-5-1-8 查看创建好的 VHD 虚拟磁盘文件

提示：可以创建一个包含四个分区的 VHD 磁盘，用于配合后续章节的实验。

3.5.2 实验 2：利用 Winhex/X-Ways Forensics 获取磁盘的物理镜像

场景：对存储介质进行证据固定。

工具准备：WinHex / X-Ways Forensics、3.5.1 实验创建的 VHD 虚拟磁盘

1.创建案件

通过文件菜单，可以创建一个新案件、打开现有案件、关闭当前案件；备份并压缩案件目录至 ZIP 文档(只适应小于 4 GB 的文件)；自动创建案件报告；将存储介质或镜像文件加入案件。

命名案件后，案例目录下会生成一个与案件同名的子目录，用于保存案例数据。在案件分析过程中，该目录下会自动生成所需的子目录。此过程完全由软件自己控制，只需注意选择好保存位置和案件名称即可。分析过程中，用户无需特意地保存案件，当最后关闭案件或退出程序是，软件会自动保存案件。

利用 WinHex / X-Ways Forensics 进行数据获取，或者进行数据分析，首先要创建一个新的案件。创建案件是为了将案件信息和需要分析的存储介质或者镜像文件加载到案例中。WinHex / X-Ways Forensics 软件本身不会使数据内容产生变化，但操作系统和应用程序则可能对新加入的设备造成数据修改。因此数据获取过程中，应注意使用硬件写保护设备。创建案件，**选择“案件数据”-点击“文件”-选择“创建案件”。**

图 3-5-2-1 创建新案件

在属性对话框中，可输入案件名称、案件描述、调查员、机构地址等辅助信息。案件名称可以根据需要设定一个便于记忆和区分的名字。**案件名称需使用英文或数字，否则将来的案例日志和案件报告中无法出现屏幕快照图片。**

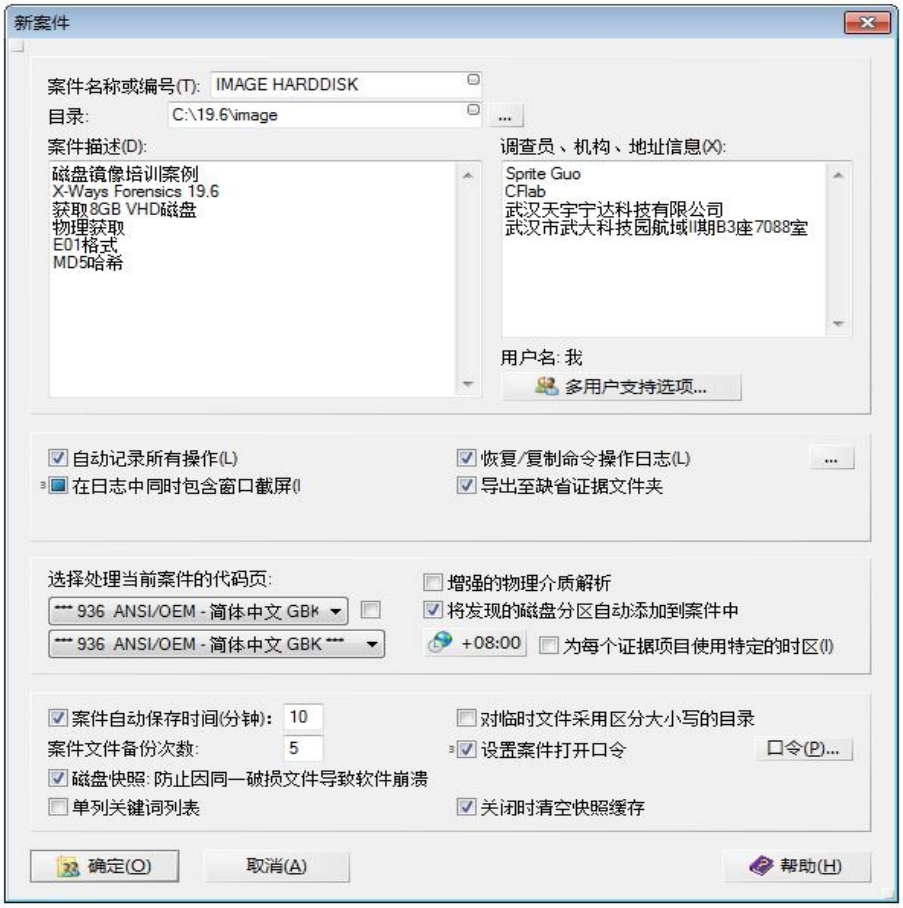

图 3-5-2-2 案件信息

WinHex / X-Ways Forensics 依据系统时钟自动生成案件创建日期。为保障 WinHex / X-Ways Forensics 在证据固定过程中记录的时间准确，且在日后数据分析过程中显示的时间正确，请核对当前计算机系统时间设置无误，并在**显示时区**中设置正确的时区信息。调查员可以通过点击**“记录所有操作”**以启用或禁用自动日志功能。当前创建的案件目录将被默认为数据恢复、证据导出的保存目录。如果需要将不同的案件中的证据文件导出到同一个目录下，可以禁用**“输出至缺省证据文件夹”**选项。

调查员可以根据案件来源地为案件设定两个不同的代码页。设定的代码页用于对案件中文件名称的支持，例如保存邮件时自动命名.eml 文件，解压缩 Zip 文件时将文件名自动转换为 Unicode。如果代码页设置错误，则文件名无法正常识别。 如两个代码相同，不会对案件产生影响。如果代码页与当前 Windows 的代码页一致，则无需设置。

创建案例还可以设置保护口令。这并不是对案件数据进行加密，只是设置了一个打开权限。

2. 添加存储设备

创建案件后，即可添加所需获取/分析的目标。选择**案件数据-文件-添加存储设备。**

可以将与当前计算机连接的计算机存储介质，如硬盘、闪存卡、USB 存储设备、CD-ROM, DVD 等添加为所需获取/分析的目标，也可添加镜像文件或普通的文件。

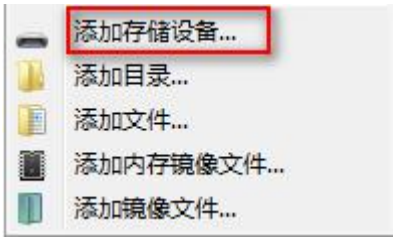

图 3-5-2-3 添加存储设备

如果需要获取某个磁盘，可以通过逻辑驱动器、物理驱动器两种方式获取。例如，磁盘中含有 C、D、E 三个分区，需以物理驱动器方式进行获取妥。本例中，我们需要对虚拟机中创立的 8GB 虚拟硬盘进行获取。首先将该硬盘加入到当前案件中。

图 3-5-2-4 选择物理驱动器

3. 创建磁盘镜像

创建磁盘镜像，需在**磁盘查看方式**下，选择菜单中的**“文件”-“创建磁盘镜像”**。如果发现创建磁盘镜像功能是灰色，无法调用，注意需将视图模式变为**“分区”**。

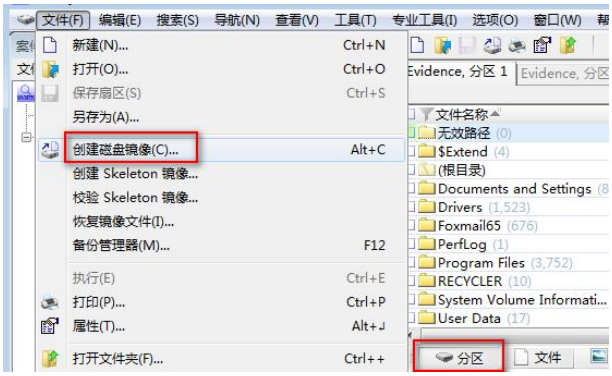

图 3-5-2-5 创建磁盘镜像-分区模式

在“创建磁盘镜像”窗口（图 3-16）中，需要注意几个方面：

1. 镜像文件格式：本例使用.E01 证据文件格式；

3. 路径和文件名：选择希望保存镜像文件的位置；

3. 设定哈希算法及校验；

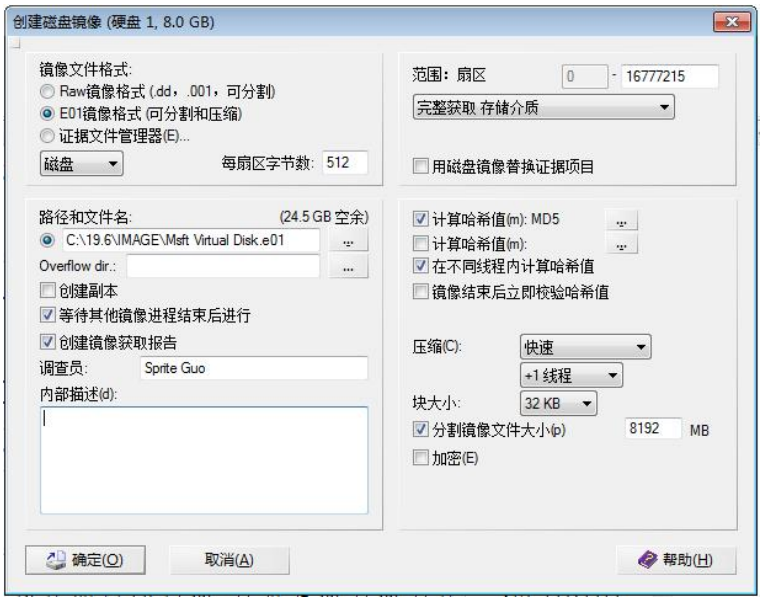

图 3-5-2-6 创建磁盘镜像

创建镜像文件过程中，将显示复制进度。请根据所作的测试镜像，填写实际获取速度比较。

E01 镜像，采用最大压缩，持续时间:_____分钟，_____MB/min；

DD 镜像， 无压缩，持续时间: _____分钟，_____MB/min；

镜像获取结束后，WinHex / X-Ways Forensics 会自动开始校验哈希值。最后显示数据获取报告。

4. 查看数据获取报告

数据获取报告是获取证据的重要依据，需妥善保存。报告中会包含如获取时间、获取工具、存储介质参数、MD5、SHA 值等信息。

数据获取报告应与磁盘镜像文件一并刻录光盘保存。数据获取结束后，应立即连接打印机，打印此报告，并由调查人员和第三方证人签字。为保持证据链的连续性，同时应填写“证据链记录表”，对各种信息记录备案，并由调查人员签字。

3.5.3 实验 3：《电子数据取证》第三章课后习题

场景：添加镜像文件，查看镜像信息。

工具准备：在本练习需要使用“B02-thumbimage_fat.dd”镜像文件。镜像文件保存于位于教学环境的“实

训案例\Part-B-File System”目录下。

问题 1：计算哈希值

问题 2：搜索关键字“Wikipedia”，当编码为 ASCII 格式时，命中次数是多少？注意，在本次练习中无需区分关键字大小写。

问题 3：关键词结果所在数据单元的编号(或地址)是什么？

问题 4：当搜索关键字编码为 Unicode 时，搜索命中数是多少？

从根本上说，计算机只会处理数字，特别是只会处理二进制数字。在存储字母和各种字符时，计算机会为每个字符分配一个数字。换句话说，所有的字母和字符必须采取一种标准方式进行编码才可以被识别出来，ASCII——美国信息交换标准代码(ISO 14962:1997)，就是一种最常见的字符编码方式。ASCII 码是一种将特定的 8 位编码(即长度为 8 位的 0 和 1 的组合)分配给字母、数字和标点符号的一种编码规则。ASCII 规定每个字符只使用 1 个字节，而 1 个字节只能表示 256 个符号。然而，世界上有许多种语言，它们会有自己的字母，或有特色的标音字符版本的 ASCII 罗马字母。显然，每个字符 8 位的方式不足以表达所有的字符,因此后来出现来一些多字节字符编码标准。目前一种非常流行的双字节(16 位)编码标准称为“Unicode”，它可以表示 65,000 多个字符(2 的 16 次方)。换句话说，Unicode 是一种可以包含世界上现存所有语种的字符编码。

1. 创建案件

参考 3.5.2 操作步骤。

2. 添加镜像文件

创建案件后，选择案件数据-文件-添加镜像文件。

浏览“CDF\实训案例\Part-B-File System”目录,选择“B02-thumbimage_fat.dd”镜像文件。然后点击“打开”。

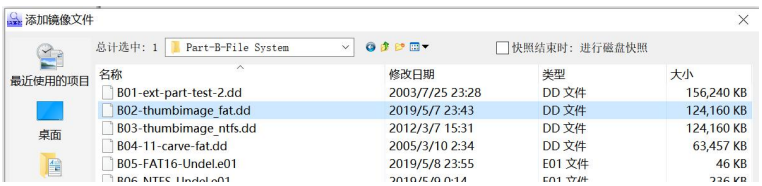

图 3-5-3-1 创建磁盘镜像

3. 计算哈希值

回答问题 1。

方法 1：利用 CDF-Hash 目录下的 Hash 工具，计算 DD 文件哈希值

方法 2：再次获取镜像，同时计算哈希值

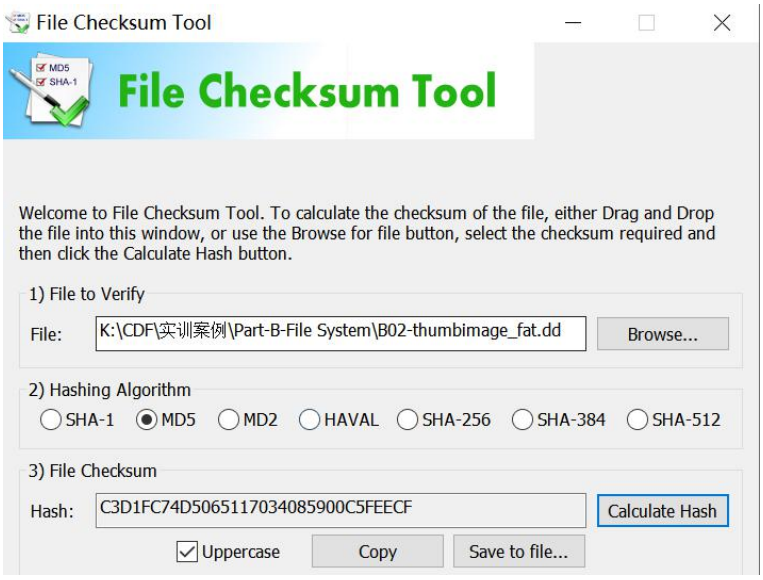

图 3-5-3-2 哈希值

4. 搜索关键词-ASCII 码

回答问题 2。

方法 1：点击“搜索”-“同步搜索”，或点击 ALT+F10。出现如下窗口，输入“Wikipedia”。如图，勾选 ASCII 码。点击“确定”。

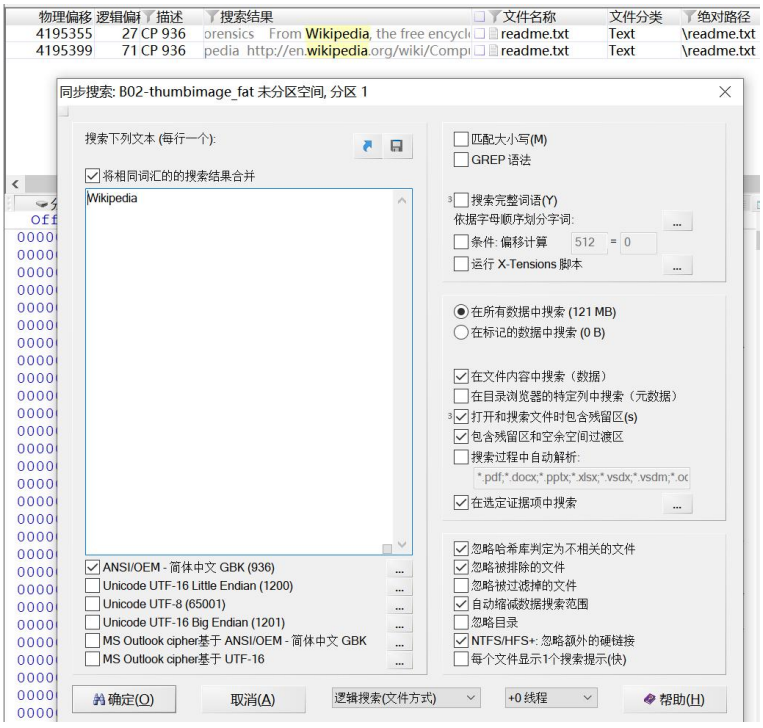

图 3-5-3-3 搜索关键词

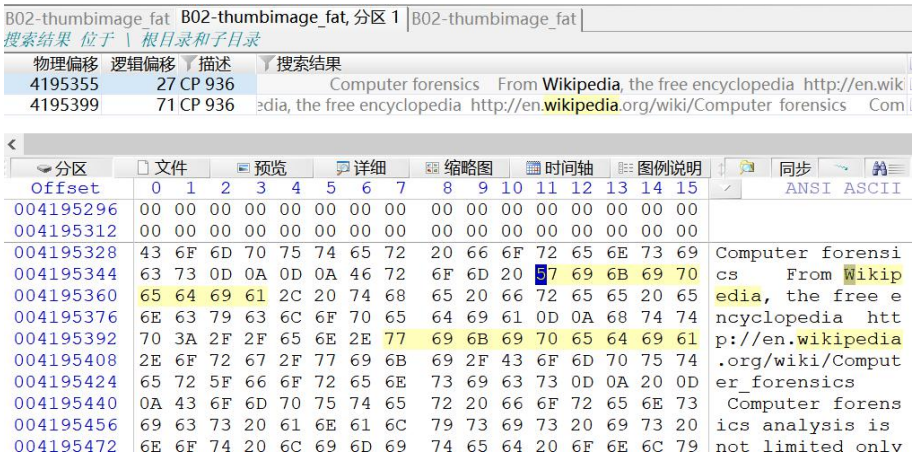

图 3-5-3-4 关键词搜索结果

5.搜索关键词-UNICODE 码

回答问题 3。

方法 1：点击“搜索”-“同步搜索”，或点击 ALT+F10。出现如下窗口，输入“Wikipedia”，按照下图，勾选 UNICODE 编码，点击“确定”。

图 3-5-3-4 设置搜索关键词的编码

3.5.4 获取 Bitlocker 加密磁盘镜像

场景：对一个连接在笔记本计算机上的加密 U 盘进行证据固定。

工具准备：X-Ways Forensics、取证计算机、加密的 VHD 虚拟磁盘、磁盘挂载工具

具体操作步骤：

1.准备加密 VHD 磁盘，Bitlokcer 加密磁盘

创建 VHD 虚拟磁盘之后，利用 Windows 对驱动器加密。并拷贝几个目录和文件。

提示：如果在一台运行的计算机中，发现驱动器图标显示为加密状态，且处于解密状态下，则尽早对加密分区进行逻辑获取。如果卸载 U 盘，不掌握密码则无法对 U 盘进行成功解密。

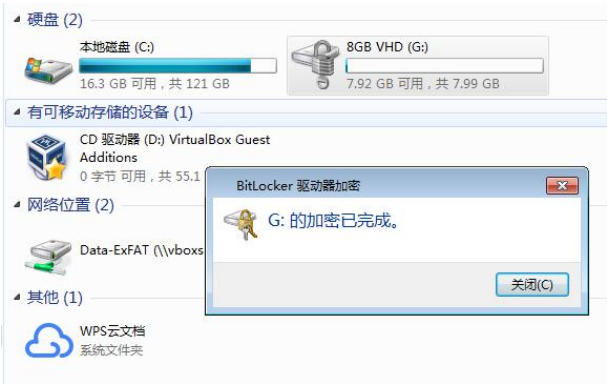

图 4-18 利用 Bitlocker 加密虚拟磁盘

2. 创建案件（参考 4.3.1）

3. 添加逻辑驱动器

本例中，我们同时添加物理磁盘和逻辑磁盘，对比物理获取和逻辑获取的区别。从图 4-19、4-20 可以看到，加载物理驱动器时，整个加密磁盘 2 个分区，可以在分区中看到一个虚拟出的 BitLocker 文件，无法看到磁盘中存储的目录和文件。加载逻辑驱动器时，可以直接查看分区，看到 X-WAYS 目录和下级文件，可以直接预览所有的文件。因此，对于处于解密状态的加密磁盘，应该通过加载逻辑驱动器方式进行磁盘镜像。

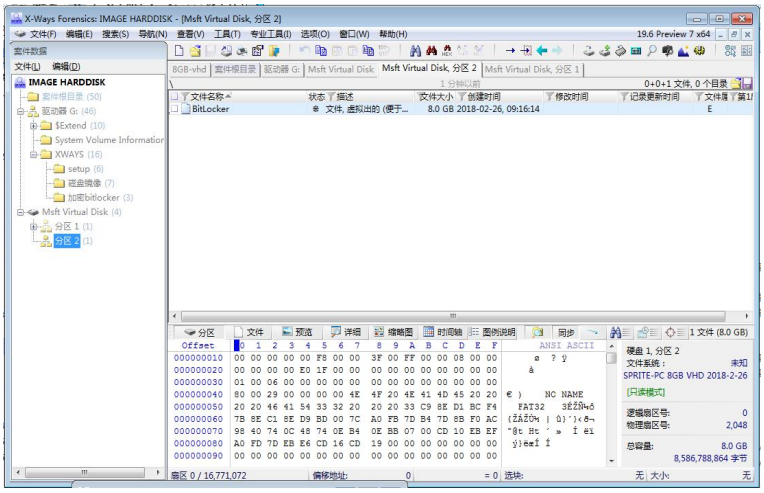

图 4-19 Bitlocker 加密后的分区

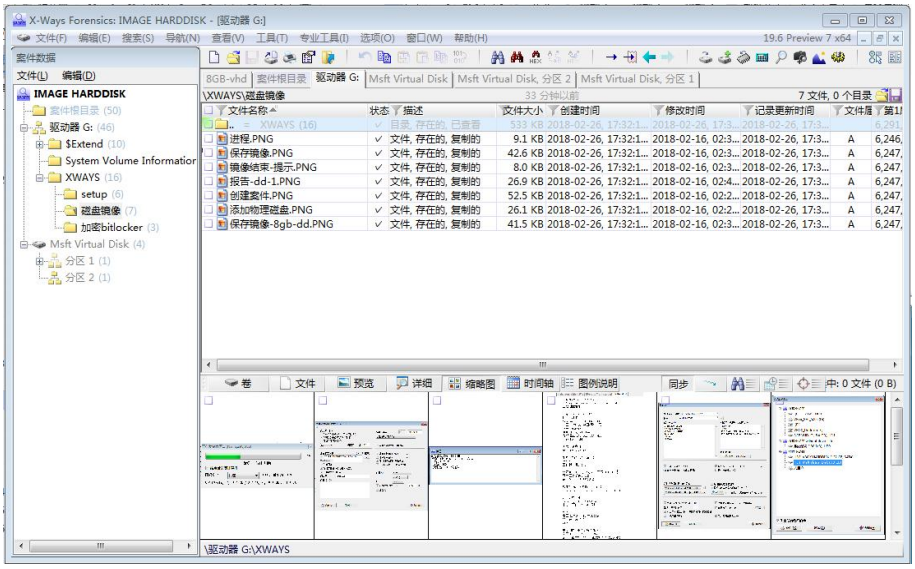

图 4-20 解密状态的 Bitlocker 分区

3.5.5 解密的 Bitlocker 磁盘镜像

场景：L12-PIC-Partition-2.e01 是一个加密的 Bitlocker 磁盘镜像。解密密钥“589215-329483-204215-213444-235455-273735-036311-409585”。现在需对 L12 镜像解密并后续进行数据恢复。

工具准备：X-Ways Forensics、磁盘挂载工具、L12-PIC-Partition-2.e01。

基本操作参考 3.5.4。本例中主要练习使用 Arsenal Image Mounter 加载 L12-PIC-Partition-2.e01 镜像文件，即可挂载出一个虚拟磁盘，例如 F。

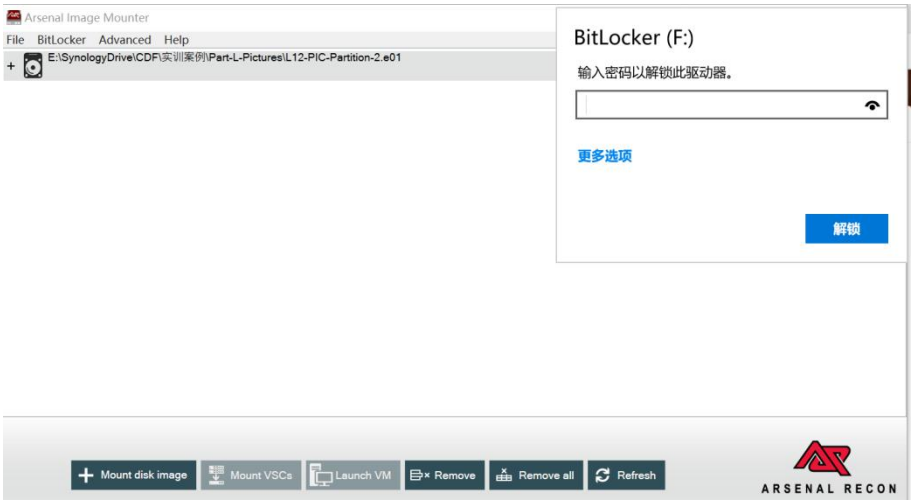

图 4-20 挂载后可以对 Bitlocker 分区进行解密

输入密钥“589215-329483-204215-213444-235455-273735-036311-409585”即可解密成功。

图 4-20 输入解密密钥进行解密

分区解密成功后，重新加载物理磁盘\逻辑磁盘，利用 X-Ways Forensics 进行数据恢复。或直接利用第三方软件对解密的分区进行数据恢复。

3.5.6 使用 DD 命令获取镜像解密的 Bitlocker 磁盘镜像

场景：L12-PIC-Partition-2.e01 是一个加密的 Bitlocker 磁盘镜像。解密密钥“589215-329483-204215-213444-235455-273735-036311-409585”。现在需对 L12 镜像解密后的分区制作 DD 镜像。

工具准备：\CDF\tools\CDF-Imager\DD64.exe

1.转换至\CDF\tools\CDF-Imager\目录下，输入命令：DD --list

2.可以看到如下显示结果

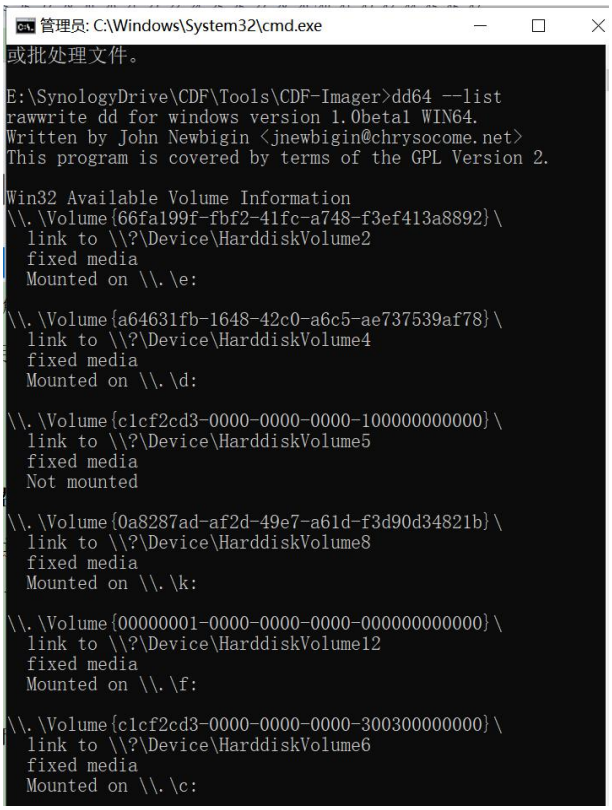

图 DD 命令识别已连接的设备

3.DD 命令参数描述

if，设定输入源，原始文件或卷

of，设定输出目标，指定的文件或卷

bs，设定块大小

size，which informs dd to determine the size of the input device and ensures dd does not read past that point. This parameter is important for external flash drives. Sometimes dd will stop working, if it attempts to read beyond the end of the volume. This feature is not enabled by default, because determining the correct size of the device is not always possible.

progress，设定镜像过程中显示当前进度

4.在命令提示符下，输入如下命令

挂载的 bitlocker 卷为 F:，将镜像保存为 c:\cdf\test\bitlocker.dd

dd64.exe if=\\.\f: of=c:\cdf\test\bitlocker.dd bs=1M --size --progress

5.开始进行镜像。结束后可以看到如下结果。

```
E:\SynologyDrive\CDF\Tools\CDF-Imager>dd64.exe if=\\.\f: of=c:\cdf\test\bitlocker.dd bs=1M --size --progress
rawwrite dd for windows version 1.0beta1 WIN64.
Written by John Newbigin <jnewbigin@chrysocome.net>
This program is covered by terms of the GPL Version 2.

2,380M
2380+1 records in
2380+1 records out

E:\SynologyDrive\CDF\Tools\CDF-Imager>
```

3.5.7 磁盘镜像

实训案例：PART-C-Windows Forensics\C01-CCFC-Windows XP.e01。 实验软件 Winhex / X-Ways Forensics，FTK Imager，猎痕磁盘挂载。注意：本练习所得答案均在未进行磁盘快照状态下完成。

题目 1

获取分区 9 的 DD 镜像，命名为“分区 9.001”，查看生成的镜像文件大小为(字节)：

A：21,638,688

B：21,638,689

C：21,639,168

D：24,643,584

题目 2

查看 C01-CCFC-Windows XP.e01 镜像中，分区 9 原始大小为(字节)：

A：21,638,688

B：21,638,689

C： 21,639,168

D： 24,643,584

题目 3

计算分区 9 的 MD5 值最后 4 位为：

问题描述：提示：点击分区 9，右键，属性

A：6B34

B：3D2B

C：8923

D：A78C

题目 4

获取镜像时，可见显示默认获取分区 9 的扇区起止范围为：

A：0-48133

B：0-48132

C：0-48131

D：0-48139

题目 5

X-Ways Forensics 支持创建的镜像格式有：

问题描述：多选题

A：RAW 格式

B：E01

C：EXO1

D：CTR

题目 6

X-Ways Forensics 支持打开的镜像格式有：

问题描述：多选题

A：DD，OO1

B：虚拟磁盘：VHD、VDI、VMDK、VHDX

C：EO1、ExO1

D：苹果 DMG

题目 7

FTK Imager 支持创建的镜像格式有：

问题描述：多选题

A：RAW（DD）

B：SMART

C：EO1

D：AFF

题目 8

FTK Imager 支持打开的镜像和文件格式有：

问题描述：多选题

A：GHOST 备份 *.GHO

B：压缩文件 *.RAR

C：光盘镜像 *.ISO

D：苹果 *.DMG

题目 9

使用 X-Ways Forensics，可以针对以下类型数据创建镜像：

问题描述：多选题

A：物理磁盘

B：逻辑磁盘

C：文件和目录（证据文件管理器 CTR 格式）

D：内存

题目 10

利用 FTK Imager 针对目录创建镜像，可以生成以下格式的镜像文件：

A：RAW（DD）

B：SMART *.S01

C：Encase *.E01

D：FTK *.AD1

题目 11

有关 X-Ways Forensics 证据文件管理器 CTR 格式镜像，下列描述正确的是？

问题描述：多选题

A：CTR 格式镜像可以用不同的取证分析软件直接打开

B：CTR 格式镜像，可以包含文件和目录\原始创建、修改和访问时间

C：CTR 格式镜像，可以恢复其中的被删除的文件

D：CTR 格式的镜像可以转为 E01 格式文件，但这个 E01 文件不是标准的 E01 文件，利用其他取证软件可能无法查看其中保存的文件

题目 12

查看 C01-CCFC-Windows XP.e01，镜像文件中包含的 MD5 哈希值（最后 4 位）为：

问题描述：提示：镜像文件，右键，属性

A：94FC

B：A62B

C：897B

D：A78C

题目 13

查看 C01-CCFC-Windows XP.e01，镜像文件中包含原始磁盘的扇区总数为：

问题描述：提示：镜像文件，右键，属性

A：16,777,216

B：16,777,316

C：8,589,934,592

D： 9,414,027

题目 14

查看 C01-CCFC-Windows XP.e01，有关镜像的内部描述信息正确的有：

问题描述：多选题

A：镜像由 X-Ways Forensics 19.8 版本软件创建

B：制作此镜像的人员是 Sprite

C：镜像的创建时间为 UTC 2021/03/29 20:27:33

D：镜像中包含的操作系统是 Win 10 (64 bit)

题目 15

B8DDC62C3E3FD7DA0EF2C9A82F5E517BE15F32DF4DFE678CC1C8E9FBFCC77F45，是镜像文件中哪一个分区的 SHA256 值？

A：9

B：8

C：7

D：6

题目 16

利用猎痕磁盘挂载，将 C01-CCFC-Windows XP.e01 镜像文件挂载后，查看分区 3 的对应盘符，可以看到该分区下有几个目录？

A：9

B：8

C：7

D：2

题目 17

计算分区 9 的 MD5 值，同时计算题目 1 获取的镜像文件”分区 9.001“的 MD5 值。请问这两个 MD5 值是否一致？问题描述：提示：利用 C:\CDF\Tools\CDF-Hash\hashtool.EXE 计算”分区 9.001"文件的 MD5 值

A：相同

B：不同

题目 18

获取分区 9 镜像，存储为“分区 9.E01”。计算镜像文件”分区 9.E01“的 MD5 值。请问所得 MD5 值与”分区 9.001“的 MD5 值是否一致？问题描述：提示：利用 C:\CDF\Tools\CDF-Hash\hashtool.EXE 计算“分区 9.E01”文件的哈希值

A：相同

B：不同

题目 19

使用猎痕磁盘挂载软件，可以挂载的镜像文件格式有哪些？

问题描述：多选题

A：DD

B：E01

C：VHD

D：DMG