LAB 02

Thầy Mai Hoàng Đỉnh

Trường đại học FPT

Người thực hiện

Đặng Hoàng Nguyên

**Lab 2: Installing ProDiscover Basic Edition**

**Cài đặt ProDiscover**

Trên màn hình Windows, giải nén tệp ProDiscoverRelease7003Basic.zip.

Chạy file ProDiscoverRelease7003Basic.exe. Chạy với quyền admin

A screenshot of a computer

Description automatically generated with medium confidenceCài đặt với tất cả cài đặt mặc định. Khi nhìn thấy hình dưới đây, click "**Anyone who uses this computer (all users)**".

**Tải image để thử nghiệm**

Trong máy window, chúng ta sẽ tải thử một file:

[http://samsclass.info/121/proj/nps-2009-canon2-gen6.dd](https://samsclass.info/121/proj/nps-2009-canon2-gen6.dd)

Lưu ý rằng ProDiscover chỉ có thể nhận được file có đuôi **.dd**

A picture containing text, screenshot, design, graphics

Description automatically generated

**Khởi động Prodiscover**

Trên màn hình của bạn, nhấp đúp vào biểu tượng "ProDiscover Basic".

Trong " Launch Dialog ", nhập " Project Number " là 5 và " Project File Name " là **5-tên của bạn**, thay thế "tên của bạn" bằng tên riêng của bạn, như được hiển thị, ví dụ: dưới:

A screenshot of a computer dialog box

Description automatically generated with medium confidenceNhấp vào **Open**.

Đây giống như mới chỉ tạo project chứ chưa cho ổ đĩa bằng chứng vào

**Thêm ổ đĩa bằng chứng**

Từ ProDiscover menu bar, nhấn **Action**, **Add**, "**Image File...**" như hình được chỉ bên dưới:

**A screenshot of a computer

Description automatically generated**

Sau đó chọn vào file canon.dd Tại đây lưu trữ tại Desktop

Bên trái của ProDiscover, trong phần “Content Viwe”. Expand phần đó ra để có thể xem được các evidence được add vào.

Mở rộng **C:\Users\Admin\Desktop\nps-2009-canon2-gen6.dd**

Mở rộng **C:**

Mở roognj **DCIM**

Chọn **100CANON**

A screenshot of a computer

Description automatically generated with medium confidence

**Sử dụng view bằng chữ cái ASCII**

Chọn 1 trong những file bên trong Folder 100Canon. Ở bên dưới bên phải thể hiện bảng ascii giống như trong HXD bảng bên phải

A screenshot of a computer

Description automatically generated

**Xem ảnh**

Phía bên cùng bên phải, nhấp đôi vào một trong những cái ảnh

Ta có thể thấy được hình ảnh đó nó được hiển thị như bên dưới

A picture containing text, screenshot, handwriting, font

Description automatically generated

Cơ bản nó vẫn là một file JPEG nên chúng ta vẫn có thể tương tác như bình thường

**Xem những ảnh bị xóa**

Trong bản bên phải trên cùng của ProDiscover ta sẽ thấy có sự xuất hiện của những file JPEG đã bị xóa, phân biệt bằng icon có dấu X. Đó là những file đã bị xóa và phát hiện bởi ProDiscovery. Chỉ phát hiện ra, và khôi phục một phần chứ không khôi phục được hết

A screenshot of a computer

Description automatically generated

**Lab 2 cont: Using ProDiscover Basic Edition**

**Downloading a Sample Disk Image**

Bên trong folder zip của bài lab, ta sẽ giải nén file p15.zip lấy file p15.dd và đem ra ngoài Desktop

A screenshot of a computer

Description automatically generated with medium confidence

Chúng ta sẽ tạo project, vẫn như cũ

Trong " Launch Dialog ", nhập " Project Number " là 5 và " Project File Name " là **5-tên của bạn**, thay thế "tên của bạn" bằng tên riêng của bạn, như được hiển thị. Tại đây, em sẽ sử dụng tiếp project cũ

**Adding an Image File**

**A screenshot of a computer

Description automatically generated**

Di chuyển tới Desktop và import p15.dd vào trong ProDiscover

**Xem content trong file p15.dd**

Trong panel bên phải của ProDiscover, trong mục “Content Vierw”, expand Images

Mở rộng C:\Users\student\Desktop\p15\p15.dd

Nhấn đúp vào C:

Nội dung của ổ C: sẽ được hiển thị bên dưới

A screenshot of a computer

Description automatically generated

**Xem file DOCX**

Bên tay phải của ProDiscover, ta sẽ click chọn file **bill-of-rights.**

Khung phía dưới bên phải hiển thị nội dung tệp trong ASCII, như được hiển thị bên dưới. Vì đây là tệp .docx nên nội dung không dễ đọc ở dạng này.

A screenshot of a computer

Description automatically generated

Nếu để ý kĩ thì ta sẽ thấy đây Header của nó là PK tượng trưng cho PK Zip, vì sao file word lại là file zip ? Cơ bản vì các file office (word, powerpoint, excel) thật chất chúng là những file zip, ta có thể dễ dàng nhận ra chúng khi mở bằng 7Zip.

Double click vào file để mở tệp lên, ta sẽ thấy được file đã có thể đọc được

A screenshot of a computer

Description automatically generated

**Xem file JPG**

Bên tay phải của ProDiscover, ta sẽ click chọn file **images.** Sẽ xuất hiện một file của một con mèo.

Phía thanh bên phải dưới của ProDiscovery có magic Header là JFIF vì thế ta có thể mở được bằng file JPEG

A screenshot of a computer

Description automatically generated with medium confidence

Tuy không coi được hex của nó nhưng nhờ có chữ “JFIF” nên ta có thể dễ dàng khẳng định đây là file JPEG. Tương tự như thế với file puppy

**Sử dụng Galllery Virew:**

Click chuột phải rồi nhấn Gallery View để xem hình không cần phải open nó

A picture containing text, screenshot, display, software

Description automatically generated

A screenshot of a computer

Description automatically generated

**Xem những file đã bị xóa**

Trong panel phía bên trái, nhấp vào **“Deleted Files”** sẽ cóc hai file xuất hiện ở phía bên phải ngoài cùng như hình sau:

A screenshot of a computer

Description automatically generated

Nhấn đúp vào hình khẩu xúng, và mở, ta có thể thấy hình đã được khôi phục hoàn toàn, kể cả tên fille.File Hacker-manifest cunxgv ậy

A screenshot of a computer

Description automatically generated with medium confidence

**Xem tất cả các file**

Trong panel bên trái của ProDiscover, nhấp chọn **“All Files”**

Có một alert nói rằng **"CAUTION:...that may take some time to complete...".**

Nhấn chọn **yes**

A screenshot of a computer

Description automatically generated

Thì ngay lập tức những file đã bị delete sẽ được recover lại

A screenshot of a computer

Description automatically generated

**Xem đĩa vật lý bằng Cluster View**

Bình thường khi chúng ta muốn xem gì thì cơ bản thì chỉ cần xem Content View, Nhưng đôi khi chúng ta cũng cần xem những bytes ở trong ổ đĩa, ta có thể dung Cluster View

Ở phía bên trái của ProDiscover, trong phần “Cluster View”, nhấn dấu cộng

Sau đó double clivk vào **C:\Users\Admin\Desktop \p15.dd**

A screenshot of a computer

Description automatically generated

Tại đây ta có thể di chuyển giữa các cluster với nhau bằn cách nhấn arrow phải trái tùy theo ý muốn và sở thích của mình.

Cluster thứ 0 sẽ tại địa chỉ 110

A screenshot of a computer

Description automatically generated

Di chuyển giữa các cluster với nhau ta có thể phát hiện rằng mỗi Cluster sẽ cách biêt nhau về 200 bytes địa chỉ.

A screenshot of a computer

Description automatically generated

Bắt đầu từ cluster 1 thì address byte của nó ở 200

Trở về với Cluster 0 thì đây chính là Master Boot Record bở ì có một đoạn text được thấy trong Master boot record: "**Error loading operating system**"

A screenshot of a computer

Description automatically generated

**Xem logical drive trong Cluster view:**

Bên trái của ProDiscover, trong “Cluster View” chọn **C:** sau đó chọn Cluster 0, và nhìn vào đoạn hex và ascii bên dưới. C ở đây được gọi là ổ C nó không giống ổ vật lý chứa MBR

A screenshot of a computer

Description automatically generated

Giữa hai cluster với nhau thì chúng cách nahu 1000 bytes

A screenshot of a computer

Description automatically generated

1000 bytes hay còn được tính là 4KB đây là một cluster size bình thường cho một ổ NTFS. Để kiếm chứng cho phần NTFS này, chúng ta sẽ kiểm tra Cluster 0 xem nó là gì. Tại vì Cluster 0 được gọi là Partition Boot Sector

Theo đúng suy đoán, đây là một ổ để format NTFS

A screenshot of a computer

Description automatically generated with medium confidence