

LAB 06
MINI PROJECT



Họ tên và MSSV: Trương Quang Long B2203727

Nhóm học phần: 01

- Các sinh viên bị phát hiện sao chép bài của nhau sẽ nhận 0đ cho tất cả bài thực hành của môn này.
- Bài nộp phải ở dạng PDF, hình minh họa phải rõ ràng chi tiết. Hình minh họa chỉ cần chụp ở nội dung thực hiện, không chụp toàn màn hình.

1. Mô tả vấn đề

Beat Step là công ty sản xuất hiệu ứng âm thanh cho các chương trình truyền hình và phim nổi tiếng. Hai trong số các tập tin âm nhạc của Beat Step đã bị đánh cắp khỏi công ty và phát tán qua Internet:

- Một tập tin có bản quyền sẽ được sử dụng trong một bộ phim sắp được phát hành.
- Tập tin còn lại không có bản quyền nhưng cần được giữ bí mật.

Beat Step đã thuê bạn (nhân viên điều tra) để xác định ai đã lấy và phát tán các tập tin và làm thế nào họ có thể làm được điều đó. Công ty đã cung cấp cho bạn:

- Tập tin 'Contraband.mp3' có chữ ký nhị phân và là tệp có bản quyền. Tập tin này đã được lên kế hoạch đưa vào bộ phim sắp phát hành.
- Tập tin 'Sample-1.mp3' không có chữ ký nhị phân và không phải là tập tin có bản quyền. Tuy nhiên, tập tin đã được lên kế hoạch trình bày trong một cuộc họp sắp tới.
- Giá trị băm MD5 và SHA1 của 2 tập tin được cung cấp.
- Dữ liệu trên ổ cứng và bộ nhớ trên máy tính của nhân viên bị tình nghi (Kamryn Allen) đã được thu thập và cung cấp.

File dữ liệu ổ cứng	Link: https://www.dropbox.com/s/1fop1ooadb2yshu/Disk_Image_ID-20210327.001 MD5: 0ADF1F182AAB391D7042133BB55CF832 SHA1: 36186D7ABC2AB6DFB783F0283E96566DB8C0B31C
File dữ liệu bộ nhớ	Link: https://www.dropbox.com/s/0rxqi65v62njd6v/Memory_Dump_ID-20210327.raw MD5: EB741D12F5D4F57D4C1D5962BEBB5771 SHA1: 59BFE8D18C1E3DCD5A4FFE920ADEA39EC3257E87
Contraband.mp3	MD5: F9D82438ED446E43CBD06ADF74BC875B SHA1: CCE250D81A2397A4B347B78337219F078DCD4E08

Sample-1.mp3	MD5: B387E8334B3DB0346CDFA14511F6913D SHA1: 23181F3D97A836106AAE5DB86B22BC34D4B1C138
--------------	---

Mục tiêu của bạn:

- Chứng minh (hoặc bác bỏ) nhân viên Kamryn đã tải xuống các tập tin .mp3.
- Nếu tìm thấy các tập tin, hãy chứng minh (hoặc bác bỏ) rằng tập tin đó có nguồn gốc từ công ty.
- Xác định cách Kamryn có được các tập tin .mp3 (nếu tìm thấy).
- Hãy tìm mọi phương pháp mà Kamryn đã tải xuống/chia sẻ các tập tin với người khác.
- Xác định xem có nghi phạm nào khác có thể có các tập tin này hay không.

2. Điều tra với Autopsy

- 2.1. Tải và cài đặt công cụ [Autopsy](#) trên máy tính cá nhân
- 2.2. Tải file dữ liệu ổ cứng máy tính của Kamryn Allen, được file Disk_Image_ID-20210327.001
- 2.3. Sử dụng công cụ Autopsy, chọn chức năng “New Case”. Nhập các thông tin cần thiết. Ở mục “Select Data Source Type” chọn “Disk Image or VM file”. Ở mục “Select Data Source” chỉ đường dẫn đến tập tin Disk_Image_ID-20210327.001 ở Câu 2.3. Ở mục “Configure Ingest Modules” chọn “Recent activity”, “Hash lookup” và “Email Praser”.
- 2.4. Sau khi Autopsy phân tích xong dữ liệu (tốn nhiều thời gian):
 - 2.4.1. Xem thông tin ở mục Operating System Information để xác định máy tính này là của Kamryn.
Chụp hình minh họa kết quả thực hiện.
Chủ sở hữu máy tính (Owner) là Kamryn. Từ thông tin này có thể xác định máy tính của Kamryn.

Path	Product ID	Owner	Data Source
C:\Windows	00326-10000-00000-AA274	Kamryn	Disk_Image_ID-20210327.001

Type	Value
Name	DESKTOP-E4SUNT2
Program Name	Windows 10 Home
Processor Architecture	AMD64
Temporary Files Directory	%SystemRoot%\TEMP
Path	C:\Windows
Product ID	00326-10000-00000-AA274
Owner	Kamryn
Source File Path	/img_Disk_Image_ID-20210327.001
Artifact ID	-9223372036854775619

- 2.4.2. Xem thông tin ở mục Recent Documents để xác định Kamryn có những hoạt động đáng ngờ liên quan đến 2 tập tin Contraband.mp3 và Sample-1.mp3

Chụp hình minh họa kết quả thực hiện.





















Kamryn đã có một số hoạt động đáng ngờ liên quan đến 2 tập tin Contraband.mp3 và Sample-1.mp3.

Source Name	S	C	O	Path	Date Accessed	Data Source
List-3.lnk				C:\Users\Kamryn\Document...	2021-03-22 03:26:41 ICT	Disk_Image_ID-20210327.001
Captures.lnk				E:\Tools\Magnet_Forensics\...	2021-03-22 00:36:45 ICT	Disk_Image_ID-20210327.001
Contraband.lnk				C:\Users\Kamryn\Download...	2021-03-27 21:25:45 ICT	Disk_Image_ID-20210327.001
Contraband.mp3.lnk				C:\Users\Kamryn\Download...	2021-03-27 21:10:00 ICT	Disk_Image_ID-20210327.001
Documents.lnk				C:\Users\Kamryn\Documents	2021-03-22 03:25:34 ICT	Disk_Image_ID-20210327.001
Downloads.lnk				C:\Users\Kamryn\Downloads	2021-03-22 03:40:28 ICT	Disk_Image_ID-20210327.001
ID-20210321.lnk				E:\Tools\Magnet_Forensics\...	2021-03-22 00:36:45 ICT	Disk_Image_ID-20210327.001
ID-20210327.lnk				E:\Tools\Magnet_Forensics\...	2021-03-27 21:21:21 ICT	Disk_Image_ID-20210327.001
List-1.lnk				C:\Users\Kamryn\Document...	2021-03-22 03:25:45 ICT	Disk_Image_ID-20210327.001
List-2.lnk				C:\Users\Kamryn\Document...	2021-03-22 03:26:16 ICT	Disk_Image_ID-20210327.001
ms-gamingoverlay---.lnk				No preferred path found	2021-03-27 09:37:13 ICT	Disk_Image_ID-20210327.001
ms-gamingoverlay-kglcheck-.lnk				No preferred path found	2021-03-10 07:39:02 ICT	Disk_Image_ID-20210327.001
Pictures.lnk				C:\Users\Kamryn\Pictures	2021-03-22 03:20:49 ICT	Disk_Image_ID-20210327.001
Reference.lnk				C:\Users\Kamryn\Document...	2021-03-22 03:25:34 ICT	Disk_Image_ID-20210327.001
Sample-1.lnk				C:\Users\Kamryn\Download...	2021-03-22 03:40:28 ICT	Disk_Image_ID-20210327.001
Sample-1.mp3.lnk				C:\Users\Kamryn\Download...	2021-03-22 03:42:38 ICT	Disk_Image_ID-20210327.001
The Internet.lnk				No preferred path found	2021-03-10 07:39:02 ICT	Disk_Image_ID-20210327.001
Torrent-Sources.lnk				C:\Users\Kamryn\Download...	2021-03-27 21:25:45 ICT	Disk_Image_ID-20210327.001
Torrents.lnk				C:\Users\Kamryn\Download...	2021-03-22 03:42:38 ICT	Disk_Image_ID-20210327.001
wallpaperflare.com wallpaper.lnk				C:\Users\Kamryn\Pictures\w...	2021-03-22 03:20:49 ICT	Disk_Image_ID-20210327.001
Sample-1.mp3.torrent.lnk				C:\Users\Kamryn\Download...	0000-00-00 00:00:00	Disk_Image_ID-20210327.001
No preferred path found.lnk				No preferred path found	0000-00-00 00:00:00	Disk_Image_ID-20210327.001
Contraband.mp3.torrent.lnk				C:\Users\Kamryn\Download...	0000-00-00 00:00:00	Disk_Image_ID-20210327.001
Sample-1.mp3.lnk				C:\Users\Kamryn\Download...	0000-00-00 00:00:00	Disk_Image_ID-20210327.001
List-3.txt.lnk				C:\Users\Kamryn\Document...	0000-00-00 00:00:00	Disk_Image_ID-20210327.001
ID-20210327.raw.lnk				E:\Tools\Magnet_Forensics\...	0000-00-00 00:00:00	Disk_Image_ID-20210327.001
Contraband.mp3.lnk				C:\Users\Kamryn\Download...	0000-00-00 00:00:00	Disk_Image_ID-20210327.001

- 2.4.3. Trên menu Tools/File Search by Attributes tìm 2 tập tin Contraband.mp3 và Sample-1.mp3 trên máy tính của Kamryn, tìm bằng tên và giá trị băm.

Chụp hình minh họa kết quả thực hiện.

- + Tìm kiếm 2 tập tin bằng tên.

Name	S	C	O
 Contraband.mp3.lnk			0
 Contraband.mp3.lnk-slack			
 Contraband.mp3.torrent			0
 Contraband.mp3.torrent-slack			
 Contraband.mp3.torrent:Zone.Identifier			0
 Contraband.mp3			0
 Contraband.mp3-slack			
 Contraband.mp3			0
 Contraband.mp3-slack			
 Contraband.mp3.torrent			0
 Contraband.mp3.torrent-slack			
 Contraband.mp3.torrent:Zone.Identifier			0
 Contraband.mp3			0
 Contraband.mp3			0
 Contraband.mp3.torrent			0
 Contraband.mp3			0
 Contraband.mp3.torrent.lnk			0
 Contraband.mp3.torrent.lnk			0
 Contraband.mp3.lnk			0
 Contraband.mp3.lnk			0

Name	S	C	O
Sample-1.mp3.lnk			0
Sample-1.mp3.lnk-slack			
Sample-1.mp3.torrent			0
Sample-1.mp3.torrent-slack			
Sample-1.mp3			0
Sample-1.mp3-slack			
Sample-1.mp3:Zone.Identifier			0
Sample-1.mp3			0
Sample-1.mp3-slack			
Sample-1.mp3:Zone.Identifier			0
Sample-1.mp3			0
Sample-1.mp3-slack			
Sample-1.mp3:Zone.Identifier			0
Sample-1.mp3.torrent			0
Sample-1.mp3.torrent-slack			
Sample-1.mp3			0
Sample-1.mp3			0
Sample-1.mp3			0
Sample-1.mp3			0
Sample-1.mp3.torrent.lnk			0
Sample-1.mp3.lnk			0
Sample-1.mp3.torrent.lnk			0
Sample-1.mp3.lnk			0

+ Tìm kiếm 2 tập tin bằng giá trị băm.

Name	S	C	O	Modified Time	Change Time
nsmail.tmp			0	2021-03-27 21:34:58 ICT	2021-03-27 21:34:58 ICT
Contraband.mp3			0	2021-03-27 21:13:44 ICT	2021-03-27 21:16:51 ICT
Contraband.mp3			0	2021-03-27 21:13:44 ICT	2021-03-27 21:25:44 ICT
Contraband.mp3			0	0000-00-00 00:00:00	0000-00-00 00:00:00
Contraband.mp3			0	0000-00-00 00:00:00	0000-00-00 00:00:00
Contraband.mp3			0	0000-00-00 00:00:00	0000-00-00 00:00:00

Name	S	C	O	Modified Time	Change Time
nsmail-1.tmp			0	2021-03-27 21:34:58 ICT	2021-03-27 21:34:58 ICT
Sample-1.mp3			0	2021-03-22 03:40:28 ICT	2021-03-27 21:16:51 ICT
Sample-1.mp3			0	2021-03-22 03:40:28 ICT	2021-03-22 03:40:54 ICT
Sample-1.mp3			0	2021-03-22 03:40:28 ICT	2021-03-22 03:40:54 ICT
Sample-1.mp3			0	0000-00-00 00:00:00	0000-00-00 00:00:00
Sample-1.mp3			0	0000-00-00 00:00:00	0000-00-00 00:00:00
Sample-1.mp3			0	0000-00-00 00:00:00	0000-00-00 00:00:00
Sample-1.mp3			0	0000-00-00 00:00:00	0000-00-00 00:00:00

- 2.4.4. Hiển thị thông tin ở mục Text của 2 tập tin Contraband.mp3 và Sample-1.mp3 để xác nhận 2 tập tin thuộc về công ty Beat Step.

Chụp hình minh họa kết quả thực hiện.

Từ thông tin trong mục text, có thể xác nhận hai tập tin thuộc về công ty Beat Step.

Name	S	C	O	Modified Time	Change Time
nsmail.tmp			0	2021-03-27 21:34:58 ICT	2021-03-27 21:34:58 ICT
Contraband.mp3			0	2021-03-27 21:13:44 ICT	2021-03-27 21:16:51 ICT
Contraband.mp3			0	2021-03-27 21:13:44 ICT	2021-03-27 21:25:44 ICT
Contraband.mp3			0	0000-00-00 00:00:00	0000-00-00 00:00:00
Contraband.mp3			0	0000-00-00 00:00:00	0000-00-00 00:00:00
Contraband.mp3			0	0000-00-00 00:00:00	0000-00-00 00:00:00

Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations

Strings
Indexed Text
Translation

Page: 1 of 2
Page
Go to Page:

Info
 !!%(+/2559<@CCFJMMPTWWZ^aaehkcoruuy|
 .! ΔME3 97
 Created by Beat Step
 h\(*1

Name	S	C	O	Modified Time	Change Time
nsmail-1.tmp			0	2021-03-27 21:34:58 ICT	2021-03-27 21:34:58 ICT
Sample-1.mp3			0	2021-03-22 03:40:28 ICT	2021-03-27 21:16:51 ICT
Sample-1.mp3			0	2021-03-22 03:40:28 ICT	2021-03-22 03:40:54 ICT
Sample-1.mp3			0	2021-03-22 03:40:28 ICT	2021-03-22 03:40:54 ICT
Sample-1.mp3			0	0000-00-00 00:00:00	0000-00-00 00:00:00
Sample-1.mp3			0	0000-00-00 00:00:00	0000-00-00 00:00:00

Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations

Strings
Indexed Text
Translation

Page: 1 of 4
Page
Go to Page:

vTPIJR
 Beat StepTYER
 2021TIT2
 New_Movie_Sample-1COMM
 Sample to be presented at upcoming meeting

- 2.4.5. Sử dụng chức năng Tools/File Search by Attributes tìm các tập tin .torrent. Trích xuất 2 tập tin Contraband.mp3.torrent và Sample-1.mp3.torrent

Chụp hình minh họa kết quả thực hiện.

Name	S	C	O	Modified Time
Contraband.mp3.torrent:Zone.Identifier			0	2021-03-27 21:10:00 ICT
Contraband.mp3.torrent:Zone.Identifier			0	2021-03-27 21:10:00 ICT
Contraband.mp3.torrent.lnk			0	0000-00-00 00:00:00
Contraband.mp3.torrent.lnk			0	0000-00-00 00:00:00
Contraband.mp3.torrent-slack				2021-03-27 21:10:00 ICT
Contraband.mp3.torrent-slack				2021-03-27 21:10:00 ICT
Contraband.mp3.torrent			0	2021-03-27 21:10:00 ICT
Contraband.mp3.torrent			0	2021-03-27 21:10:00 ICT
Contraband.mp3.torrent			0	0000-00-00 00:00:00

Name	S	C	O	Modified Time
Sample-1.mp3.torrent.lnk			0	0000-00-00 00:00:00
Sample-1.mp3.torrent.lnk			0	0000-00-00 00:00:00
Sample-1.mp3.torrent-slack				2021-03-22 03:42:39 ICT
Sample-1.mp3.torrent-slack				2021-03-22 03:42:39 ICT
Sample-1.mp3.torrent			0	2021-03-22 03:42:39 ICT
Sample-1.mp3.torrent			0	2021-03-22 03:42:39 ICT

- 2.4.6. Tải và cài đặt Torrent File Editor vào máy tính, sử dụng công cụ mở 2 tập tin Contraband.mp3.torrent và Sample-1.mp3.torrent. Trả lời vào bảng sau:

	Created by
Sample-1.mp3.torrent	uTorrent/3.5.5
Contraband.mp3.torrent	qBittorrent v4.3.3

Chụp hình minh họa kết quả thực hiện.

Name	Contraband.mp3	Comment
URL		
Publisher		
Created by	qBittorrent v4.3.3	
Date created	3/27/2021 9:05:03 PM	
Private torrent	<input type="checkbox"/>	
Piece size	16 KiB	
Pieces	2	
Total size	28.87 KiB	
Hash	894127c6ed38852d4a6ad80b1b20b59f3e974ea0	
Magnet Link	dp%3A%2F%2Ftracker.army%3A6969%2Fannounce	

Name	Sample-1.mp3	Comment
URL		
Publisher		
Created by	uTorrent/3.5.5	
Date created	3/22/2021 3:42:39 AM	
Private torrent	<input type="checkbox"/>	
Piece size	16 KiB	
Pieces	4	
Total size	63 KiB	
Hash	67e27548f5ae2456400757756373ba271812ef59	
Magnet Link	ttp%3A%2F%2F54.37.106.164%3A80%2Fannounce	

2.4.7. Sử dụng công cụ [Torrent File Editor](#) mở tập tin resume.dat. Tới thẻ Tree, lần lượt ở mục Contraband.mp3.torrent và Sample-1.mp3.torrent, đến mục peers6 trích xuất thông tin và trả lời vào bảng sau:

	Giá trị HEX	Địa chỉ IP (DEC)	Cổng (DEC)
Sample-1.mp3.torrent	0a 00 02 0f ba3c	10.0.2.15	15546
	7f 00 00 01 ba3c	127.0.0.1	15546
Contraband.mp3.torrent	0a 00 02 0f ba3c	10.0.2.15	15546

	7f 00 00 01 ba3c	127.0.0.1	15546
	49 d4 68 e9 51c7	73.212.104.233	51025
	45 8f 19 7e ba3c	69.143.25.126	15546


Chụp hình minh họa kết quả thực hiện.



	Type	Hex	Value
> observers	list		
order	integer		-1
outofspace	integer		0
override_seedsettings	integer		0
parent_info	string	<input type="checkbox"/>	
path	string	<input type="checkbox"/>	C:\Users\Kamryn\Downloads\Cont...
peers6	string	<input checked="" type="checkbox"/>	00000000000000000000ffff0a00020...
prio	string	<input type="checkbox"/>	

	Type	Hex	Value
order	integer		-1
outofspace	integer		0
override_seedsettings	integer		0
parent_info	string	<input type="checkbox"/>	
path	string	<input type="checkbox"/>	C:\Users\Kamryn\Downloads\Sam...
peers6	string	<input checked="" type="checkbox"/>	00000000000000000000ffff0a00020...
prio	string	<input type="checkbox"/>	

Sử dụng trang <https://www.iplocation.net/> để tìm vị trí của các IP trên.

Chụp hình minh họa kết quả thực hiện.












Geolocation data from		IP2Location	Product: DB6, 2024-11-1
	IP ADDRESS:	73.212.104.233	 ISP: Comcast Cable Communications LLC
	COUNTRY:	United States 	 ORGANIZATION: Not available
	REGION:	Maryland	 LATITUDE: 39.2904
	CITY:	Baltimore	 LONGITUDE: -76.6122

Geolocation data from		IP2Location	Product: DB6, 2024-11-1
	IP ADDRESS: 69.143.25.126		ISP: Comcast Cable Communications LLC
	COUNTRY: United States 		ORGANIZATION: Not available
	REGION: Maryland		LATITUDE: 39.0841
	CITY: Rockville		LONGITUDE: -77.1529

2.4.8. Ở mục E-Mail Messages tìm thông tin các email và trả lời vào bảng sau: tên người đã gửi cho Kamryn tập tin Contraband.mp3.torrent và Sample-1.mp3.torrent và 2 địa chỉ email đã được Kamryn gửi 2 tập tin trên. Trả lời vào bảng sau:

Thời gian	Chủ đề email	Địa chỉ email gửi	Địa chỉ email nhận
2021-03-21 23:19:12 ICT	Try this one!	willis.gibbs@outlook.com	kamalle123@outlook.com
2021-03-27 21:09:14 ICT	Here's Another One	willis.gibbs@outlook.com	kamalle123@outlook.com
2021-03-27 21:34:58 ICT	Check these files out!	kamalle123@outlook.com	realltrain@gmail.com; ram91284@hotmail.com

Chụp hình minh họa kết quả thực hiện.

Source Name	S	C	O	E-Mail From	E-Mail To	Subject	Date Received
 Sent-1				kamalle123@outlook.com;	willis.gibbs@outlook.com;	Re: Try this one!	2021-03-22 03:32:56 ICT
 Sent-1				kamalle123@outlook.com;	willis.gibbs@outlook.com;		2021-03-22 03:32:56 ICT
 INBOX				willis.gibbs@outlook.com;	kamalle123@outlook.com;	Try this one!	2021-03-21 23:19:12 ICT
 Sent-1				kamalle123@outlook.com;	willis.gibbs@outlook.com;	Re: Try this one!	2021-03-22 03:32:56 ICT
 Sent-1				kamalle123@outlook.com;	willis.gibbs@outlook.com;		2021-03-27 21:26:59 ICT
 Sent-1				kamalle123@outlook.com;	willis.gibbs@outlook.com;	Re: Here's Another One	2021-03-27 21:26:59 ICT
 INBOX				email@engage.windows.com;	kamalle123@outlook.com;	Confirmation: Your Micr...	2021-03-10 12:46:31 ICT
 INBOX				willis.gibbs@outlook.com;	kamalle123@outlook.com;	Re: Try this one!	2021-03-21 23:32:03 ICT
 Sent-1				kamalle123@outlook.com;		Check these files out!	2021-03-27 21:34:58 ICT
 INBOX				willis.gibbs@outlook.com;	kamalle123@outlook.com;	Here's Another One	2021-03-27 21:09:14 ICT
 Sent-1				kamalle123@outlook.com;	realltrain@gmail.com; ram91284@hotmail.com;	Check these files out!	2021-03-27 21:34:58 ICT

2.4.9. Ở mục Web History, tìm địa chỉ trên web có Title là “New Music | Social Upload”

Chụp hình minh họa kết quả thực hiện.

History
0
https://dfir-projects.boards.net/thread/7/new-music
... New Music | Social Upload

Hex
Text
Application
Source File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annot

Result: 106 of 150
Result

Visit Details

Title: New Music | Social Upload
Username: Default
Date Accessed: 2021-03-22 03:53:19 ICT
Domain: boards.net
URL: https://dfir-projects.boards.net/thread/7/new-music
Referrer URL: https://dfir-projects.boards.net/thread/7/new-music

Source Name	URL
History	https://dfir-projects.boards.net/thread/7/new-music

- 2.4.10. Sử dụng trình duyệt web truy cập vào địa chỉ tìm được ở Câu 2.4.9. Đăng nhập vào website sử dụng tài khoản “lab/illegal_download_lab”. Download tập tin Sample-1.mp3.torrent. Sử dụng [trang sau](#) để tính giá trị băm của tập tin, so sánh giá trị tìm được với giá trị băm của tập tin máy của Kamryn.

Chụp hình minh họa kết quả thực hiện.

Giá trị băm của hai tập tin giống nhau.

New Music
Reply

« Prev
1
Next »
Actions
Search...

blowtorch
New Member
★

Mar 21, 2021 at 11:53pm
Quote

Hey guys,

This is some good music that's supposed to be released sometime in the fall or next year. Get it while you still can. [Sample-1.mp3.torrent](#) (4.52 KB)

Note: This is not a copyrighted torrent. This is for testing purposes only.

md5
16
8AC86F7A2151250BC4033FDE9E23456F