

**ITIS 5250**

**VINITHA MATHIYAZHAGAN**

**GRADUATE LAB**

**12/9/2020**

## **Overview**

On 12/9/2020, I was asked to perform forensic examination on the provided Image (**GraduateResearch.E01**) on a digital evidence of a crime story. The crime story involves a murder where there are two suspects named suspect A and suspect B in which suspect A has an Alibi. This forensic investigation begins with suspect A whose laptop has been ceased and is ready to be forensically examined. In this Lab, I will be examining suspect A's laptop where his laptop is forensically imaged, and all the analysis will be performed on this forensic image using forensic tools such as **FTK Imager 4.5.0.3**, **Autopsy 4.16.0** and **WinPrefetchView**.

## **Environment Setup:**

I started the lab by creating forensic evidence in a **Windows 8.1 Virtual Machine** and chose **VMware workstation** to deploy the Windows 8.1 Virtual Machine for this examination. I installed FTK imager on Windows 8.1 Virtual machine then used that to take forensic image of the logical drive (C:\). I exported the forensic image in. E01 format and saved it locally on my computer.

## **Software's Installed:**

**VMware Workstation Pro v15.1.1, Windows 8.1, Thunderbird, Hydra, Johnny (John the Ripper) and fcrackzip v1.0**

For creating evidence related to email communication, I downloaded Thunderbird for Windows. Hydra and Johnny (John the Ripper) were installed to brute force the password of Coffee Shop Wi-Fi. **fcrackzip v1.0** was also installed to crack the password for zipped file.

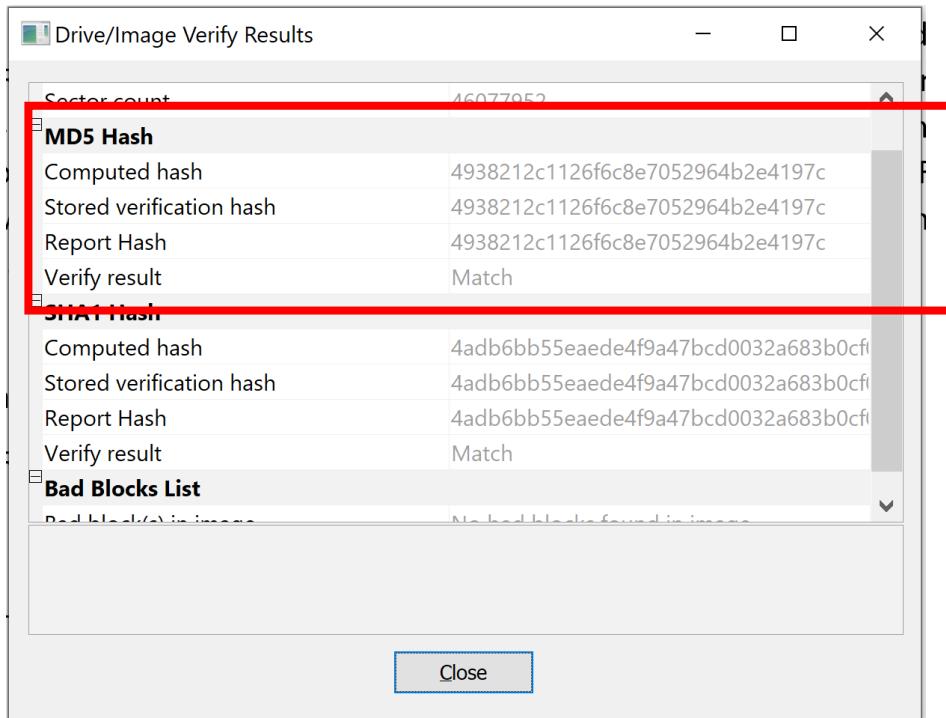
Kali Linux was also used to crack the password for zipped folder using fcrackzip and an online tool **Crack Station** was used to find the original value of the hashes found.

## Forensic Acquisition & Exam Preparation

I started my exam preparation by importing the forensically prepared image GraduateResearch.E01 in FTK Imager 4.5.0.3 and loaded the same as Disk Image in Autopsy 4.16.0 for my further analysis. I verified the hashes of both the images to ensure no interior data was tampered. I also used Autopsy 4.16.0 and WinPrefetchView for my further analysis to answer the questions given in the specified lab.

### **Hash Details:**

#### **GraduateResearch.E01**



## Findings and Report (Forensic Analysis)

Using FTK Imager 4.5.0.3 and Autopsy 4.16.0, it was possible to forensically analyze the image in detail. Each item is addressed separately below.

While analyzing the email communications using Autopsy, I found a series of them in the **Sent Folder** where Suspect A ([hashbytev@gmail.com](mailto:hashbytev@gmail.com)) has communicated via email to his friend **Cameg** ([cameg99755@hmnnmw.com](mailto:cameg99755@hmnnmw.com)) about his plans of murder and has also requested him to keep some storage space for him to hide his weapons.

The screenshot shows the Autopsy Forensic Browser interface. On the left, the 'Results' pane is expanded, showing various forensic findings under 'Extracted Content' and 'E-Mail Messages'. A red box highlights the 'E-Mail Messages' section, specifically the '[Gmail] (Drafts, Sent Mail)' folder, which contains 'Drafts (2)' and 'Sent Mail (4)'. Another red box highlights the 'Sent Mail (4)' items. On the right, the main pane displays the '[Gmail]' results table, showing four sent emails from 'hashbytev@gmail.com' to 'cameg99755@hmnnmw.com' with subject lines related to help and storage. Below the table, a specific email message is reconstructed:

From: hashbytev@gmail.com  
To: cameg99755@hmnnmw.com  
CC:  
Subject: HELP me with some space for storage

Headers Text HTML RTF Attachments (0) Accounts

Hey Cameg,  
Hashbyte here.  
  
I need your help man! Please make some space at your place for me to store some stuffs.  
  
I will explain you everything about my stuffs in coming days.  
  
"Its revenge time!"  
  
Thanks,  
Hashbyte

There were also few images attached to an email explaining about **his stuffs for identification**.

The screenshot shows a digital forensics interface displaying an email message. The top header bar includes tabs for 'Sent Mail' (with two entries), 'hashbytev@gmail.com;', 'cameg99755@hmnnmw.com;', and 'Kill Time'. Below this is another row with 'Sent Mail', 'hashbytev@gmail.com;', 'cameg99755@hmnnmw.com;', and 'Here are the st'. A navigation bar below the header includes 'Hex', 'Text', 'Application', 'File Metadata', 'Context', 'Results', 'Annotations', and 'Other Occurrences'. The 'Results' tab is selected, showing 'Result: 6 of 19'. A red box highlights the 'From:' and 'To:' fields in the message body:  
From: hashbytev@gmail.com;  
To: cameg99755@hmnnmw.com;A second red box highlights the 'Attachments (2)' tab in the message header:  
Headers Text HTML RTF **Attachments (2)** AccountsThe main message body is enclosed in a large red box:

Below I have attached the images of those stuffs which I bought for the murder.  
You gotta make some room for them and also take care of them good.  
Thanks,  
Hashbyte

Sent Mail hashbytev@gmail.com; cameg99755@hmnnmw.com; Kill  
Sent Mail hashbytev@gmail.com; cameg99755@hmnnmw.com; Her

< [REDACTED]

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Result: 6 of 19 Result ← →

From: hashbytev@gmail.com;  
To: cameg99755@hmnnmw.com;  
CC:  
Subject: Here are the stuffs!

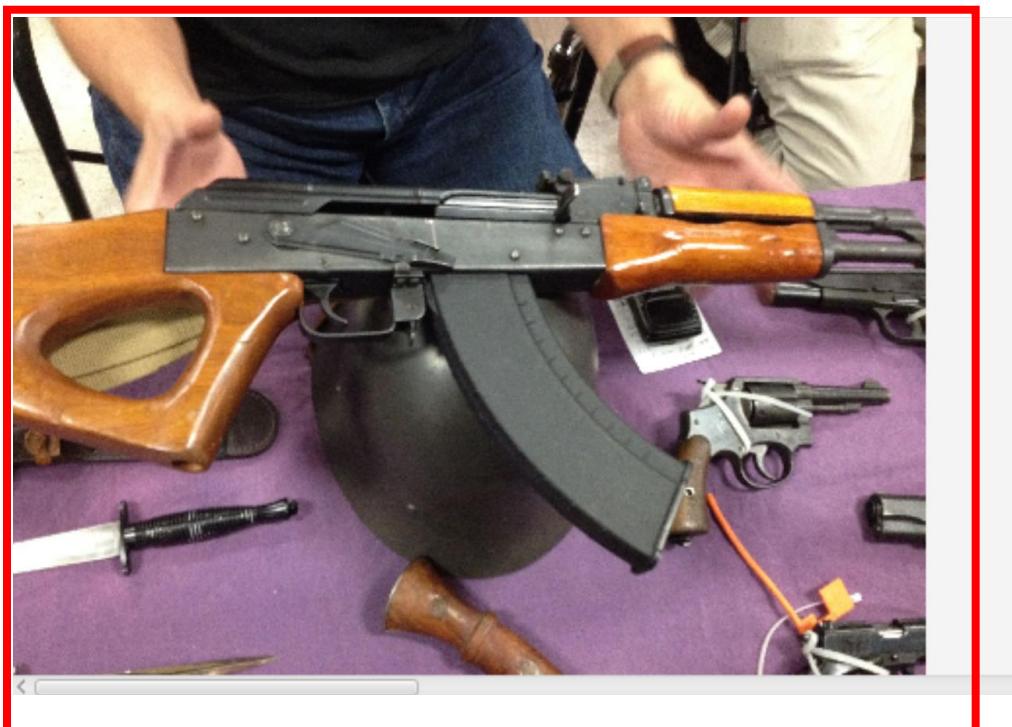
Headers Text HTML RTF Attachments (2) Accounts

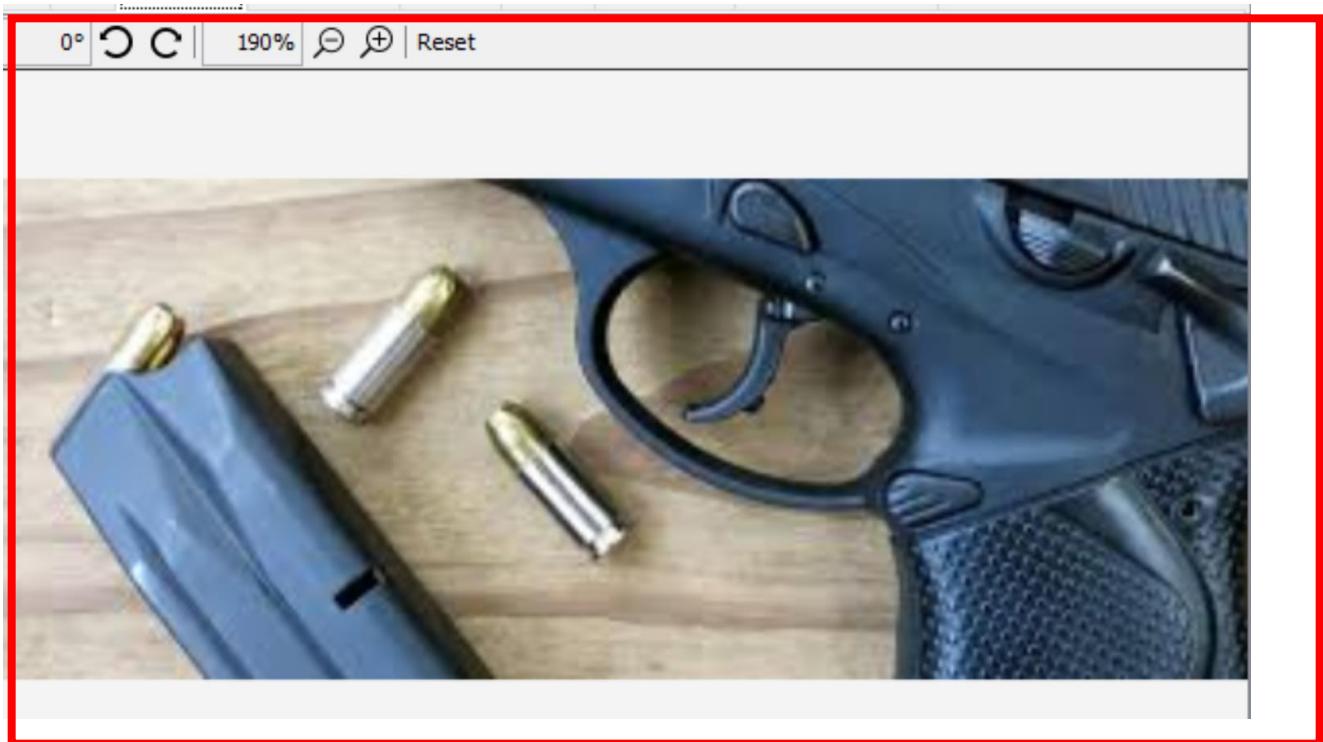
Table Thumbnail

Page: 1 of 1 Pages: ← → Go to Page: Images: 1-2 Medium


/img\_GraduateRe... /img\_GraduateRe...





Another email from Hashbyte to his friend Cameg stated some details about his Alibi. The email clearly stated that the **murder place** which he decided was **UTN (University Terrace North)** but planned to trick the police officers about informing his presence in a **Coffee Shop** during the murder time.

And he was also successful in hacking the **wifi password** and the **CCTV footage of the Coffee Shop** to place his earlier visit picture as a footage during the murder time as per his email communication.

Sent Mail | hashbytev@gmail.com; cameg99755@hmnnmw.com; Kill Time

Sent Mail | hashbytev@gmail.com; cameg99755@hmnnmw.com; Here are the stuffs!

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Result: 5 of 19 Result ← →

From: hashbytev@gmail.com;  
To: cameg99755@hmnnmw.com;  
CC:  
Subject: Kill Time

Headers Text HTML RTF Attachments (0) Accounts

Hey man!

I think you will be clear with my ideas of executing this murder plan from our yesterday's call.

You gotta take care things with cops. Let them know my whereabouts as Coffee shop and not as the murder place (University Terrace North UTN).

I somehow managed to hack the Coffee shop's CCTV footage and matched it with my previous visit. Thanks to all the open source hacking tools ;)

Thanks,

Hashbyte

In the “Deleted Folder”, there was a **FLORIDA FIREARM (GUN) BILL OF SALE** pdf file which might have been filled up by Hashbyte to buy a gun.

File: Florida-Firearm-Gun-Bill-of-Sale-Form.pdf

File Metadata: FLORIDA FIREARM (GUN) «BILL« OF SALE 1.) SELLER

Annotations: /img\_GraduateResearch.E01/Users/IEUser/AppData/Local/... 0000-00-00

Other Occurrences: /img\_GraduateResearch.E01/Users/IEUser/AppData/Roam... 0000-00-00

Other Occurrences: /img\_GraduateResearch.E01/Users/IEUser/AppData/Local/... 2020-12-11

Hex Text Application File Metadata Context Results Annotations Other Occurrences

**FLORIDA FIREARM (GUN) BILL OF SALE**

**1.) SELLER INFORMATION:**

Name: \_\_\_\_\_

Mailing Address: \_\_\_\_\_ City: \_\_\_\_\_

State: \_\_\_\_\_ Zip: \_\_\_\_\_

Driver's License Number: \_\_\_\_\_

**2.) BUYER INFORMATION:**

Name: \_\_\_\_\_

Mailing Address: \_\_\_\_\_ City: \_\_\_\_\_

State: \_\_\_\_\_ Zip: \_\_\_\_\_

Driver's License Number: \_\_\_\_\_

Page 1 / 4

There was also some CCTV footage in the “Deleted Folder”, gun and rifle pictures in “Downloads” were found using Autopsy.

File Types

- By Extension
  - Images (11146)
  - Videos (149)
  - Audio (269)
  - Archives (74)
  - Databases (88)
  - Documents
  - Executable
- By File Type
  - Deleted Files
  - File System (74240)
  - All (74240)
- File Size

Results

- Extracted Content
- EXIF Metadata (4)
- Encryption Detected (2)
- Encryption Suspected (1)
- Extension Mismatch Detected (22)
- Metadata (12)
- Operating System User Account (5)
- Recent Documents (6)
- User Content Suspected (4)
- Web Bookmarks (1)
- Web Cache (1730)
- Web Cookies (109)
- Web History (105)

Keyword Hits

- Single Literal Keyword Search (102)
- Single Regular Expression Search (0)
- Email Addresses (628)

Hashset Hits

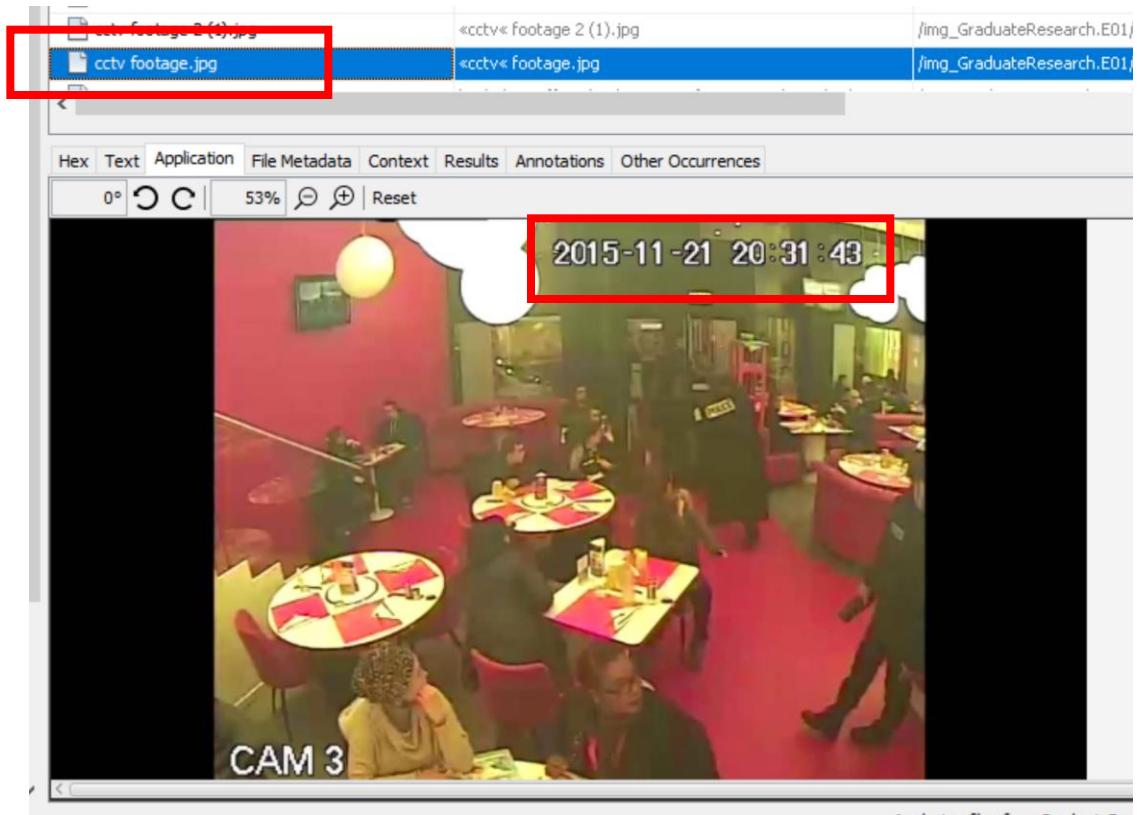
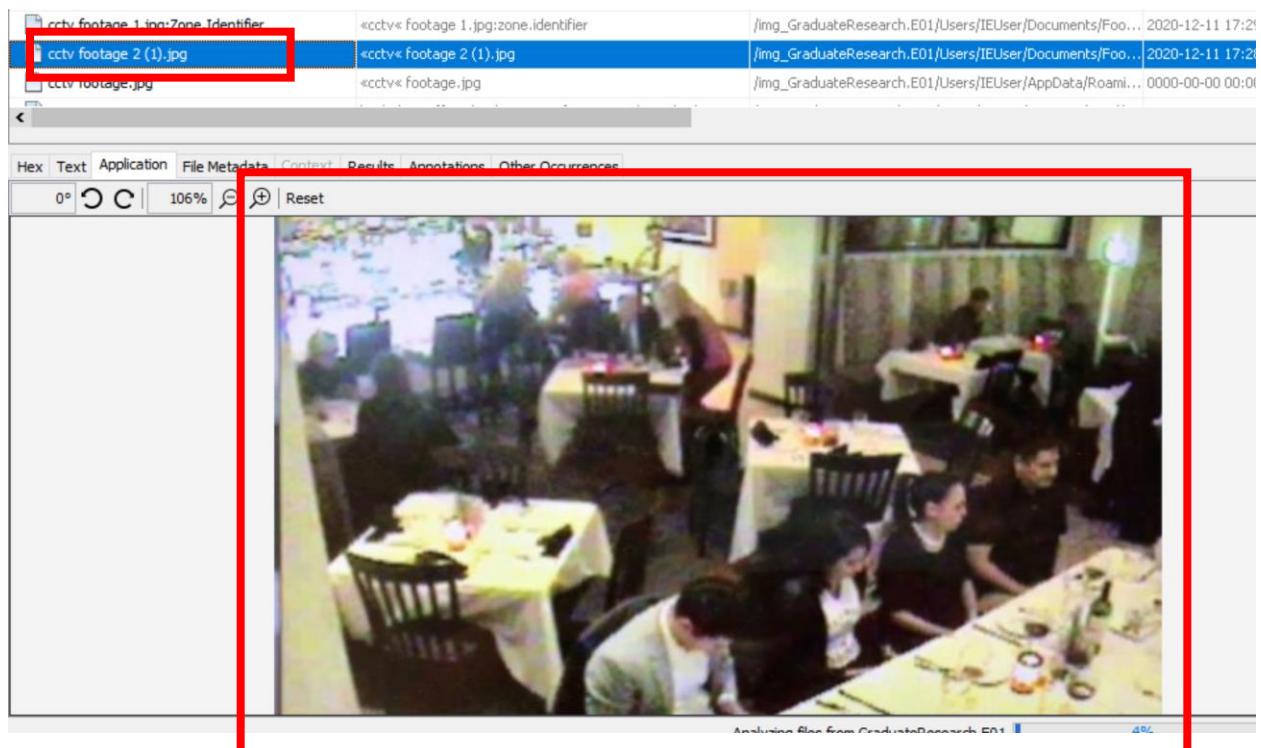
E-Mail Messages

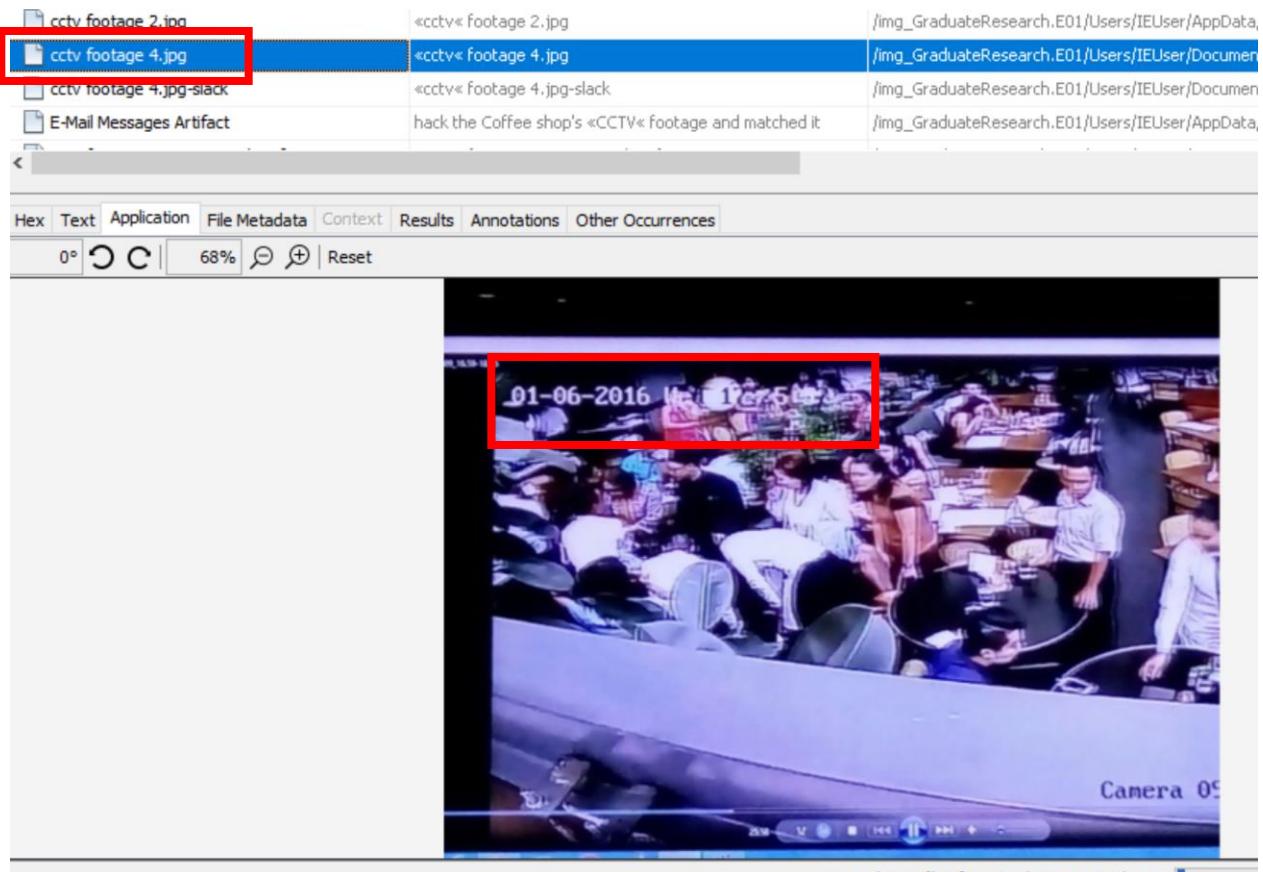
Default ([Default])

Default (3)

Name	Keyword Preview	Location
cctv footage 1.jpg	<cctv> footage 1.jpg	/img_GraduateResearch.E01/Users/IEUser/Documents/Foo... 4
cctv footage 1.jpg-slack	<cctv> footage 1.jpg-slack	/img_GraduateResearch.E01/Users/IEUser/AppData/Local/... 2
Web Cache Artifact	https://myhackingworld.com/hack-<cctv>-camera/Date Cre...	/img_GraduateResearch.E01/Users/IEUser/AppData/Local/... 2
cctv footage 1.jpg:Zone.Identifier	<cctv> footage 1.jpg:zone.Identifier	/img_GraduateResearch.E01/Users/IEUser/Documents/Foo... 2
cctv footage 2 (1).jpg	<cctv> footage 2 (1).jpg	/img_GraduateResearch.E01/Users/IEUser/Documents/Foo... 2
cctv footage.jpg	<cctv> footage.jpg	/img_GraduateResearch.E01/Users/IEUser/AppData/Roam... 0

Hex Text Application File Metadata Context Results Annotations Other Occurrences





The above date captured in the footage (which is a lot earlier) **does not match** with the recent murder date happened as per the statement provided.

### Images of Gun and Rifle in the location

[/img\\_GraduateResearch.E01/Users/IEUser/Downloads/](/img_GraduateResearch.E01/Users/IEUser/Downloads/)

/Img\_GraduateResearch.E01/Users/IEUser/Downloads

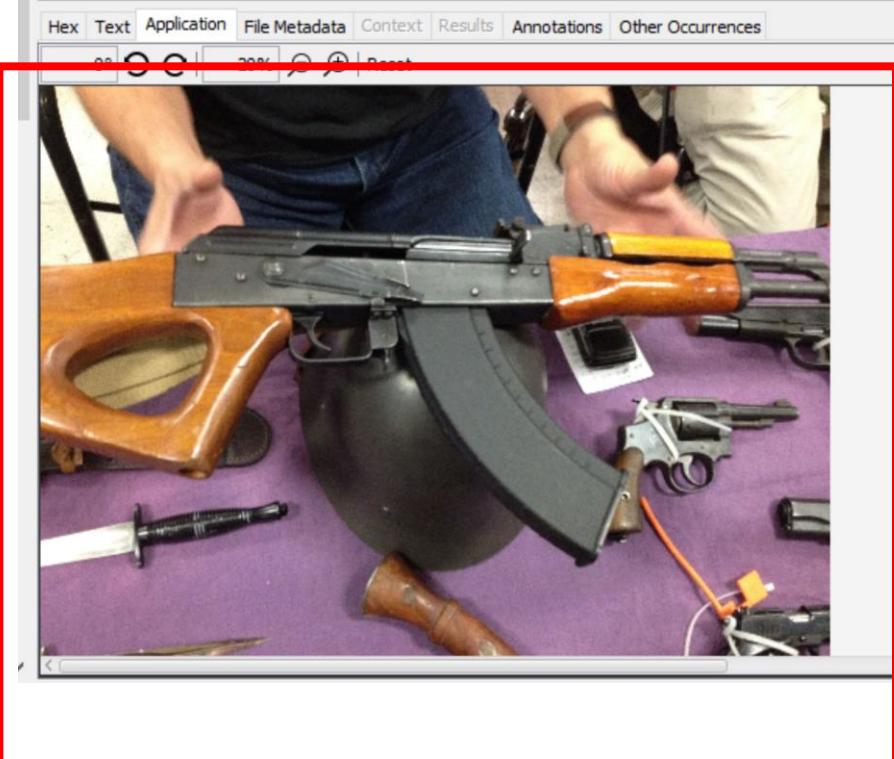
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
johnny_2_2_win.zip:Zone.Identifier	3			2020-12-11 17:36:30 EST	2020-12-11 17:36:37 EST	2020-12-11 17:36:14 EST	2020-12-11 17:36:14 EST	26
Seller_holding_rifle.JPG	1			2020-12-11 17:29:18 EST	2020-12-11 17:29:18 EST	2020-12-11 17:29:17 EST	2020-12-11 17:29:17 EST	760632
Seller_holding_rifle.JPG:Zone.Identifier	3			2020-12-11 17:29:18 EST	2020-12-11 17:29:18 EST	2020-12-11 17:29:17 EST	2020-12-11 17:29:17 EST	26
UTN_MAP.jpg	2			2020-12-11 17:29:21 EST	2020-12-11 17:30:46 EST	2020-12-11 17:29:19 EST	2020-12-11 17:29:19 EST	304253
UTN_MAP.jpg:Zone.Identifier	3			2020-12-11 17:29:21 EST	2020-12-11 17:30:46 EST	2020-12-11 17:29:19 EST	2020-12-11 17:29:19 EST	26
gun.jfif	2			2020-12-11 17:29:13 EST	2020-12-11 17:31:02 EST	2020-12-11 17:29:10 EST	2020-12-11 17:29:10 EST	9281

Hex Text Application File Metadata Context Results Annotations Other Occurrences



johnny\_2\_2\_win.zip:Zone.Identifier

Seller_holding_rifle.JPG	1	2020-12-11 17:29:18 EST	2020
Seller_holding_rifle.JPG:Zone.Identifier	3	2020-12-11 17:29:18 EST	2020
UTN_MAP.jpg	2	2020-12-11 17:29:21 EST	2020
UTN_MAP.jpg:Zone.Identifier	3	2020-12-11 17:29:21 EST	2020
gun.jfif	2	2020-12-11 17:29:13 EST	2020



In the same above location “Downloads”, there was a map found named **UTN\_MAP.jpg** to **UTN (University Terrace North)** which is the murder place as per the statement and from the above email communication from Hashbyte to his friend Cameg.

Seller_holding_rifle.JPG-Zone.Identifier	3	2020-12-11 17:29:18 EST	2020-12-11 17:29:18 EST	2020-
<b>UTN_MAP.jpg</b>	2	2020-12-11 17:29:21 EST	2020-12-11 17:30:46 EST	2020-
UTN_MAP.jpg.Zone.Identifier	3	2020-12-11 17:29:21 EST	2020-12-11 17:30:46 EST	2020-
gun.jfif	2	2020-12-11 17:29:13 EST	2020-12-11 17:31:02 EST	2020-

Hex Text Application File Metadata Context Results Annotations Other Occurrences

0° C C | 21% ⌂ ⌂ | Reset

Analyzing files from GraduateRes

An image of knife was also found in the location

/img\_GraduateResearch.E01/\$Recycle.Bin/

The screenshot shows the Autopsy forensic analysis interface. On the left is a tree view of the file system, with a red box highlighting the '\$Recycle.Bin' folder under 'Users'. Inside '\$Recycle.Bin', there is a subfolder named 'S-1-5-21-3040204872-3082932231-1584796067-1001' containing two files: '\$RE9W5TU.zip' and '\$RLAU0KM.zip'. On the right is a table view of file metadata for files in the current folder, with a red box highlighting the row for '\$RZFN1Y9L.jpg'. Below the table is a preview pane showing a photograph of a knife lying on a surface.

Name	S	C	O	Modified Time	Change Time	Access Time
\$R8W04JP.jpg:Zone.Identifier	3			2020-12-11 17:29:16 EST	2020-12-11 17:31:20 EST	2020-12-11 17:29:15 EST
\$RH6PLRB.jpg	2			2020-12-11 17:28:57 EST	2020-12-11 17:29:49 EST	2020-12-11 17:28:56 EST
\$RH6PLRB.jpg:Zone.Identifier	3			2020-12-11 17:28:57 EST	2020-12-11 17:29:49 EST	2020-12-11 17:28:56 EST
\$RMN5089.jpg	2			2020-12-11 17:28:51 EST	2020-12-11 17:29:49 EST	2020-12-11 17:28:50 EST
\$RMN5089.jpg:Zone.Identifier	3			2020-12-11 17:28:51 EST	2020-12-11 17:29:49 EST	2020-12-11 17:28:50 EST
\$RQ7Y9ZM.jpg	2			2020-12-11 17:29:00 EST	2020-12-11 17:29:49 EST	2020-12-11 17:28:59 EST
\$RQ7Y9ZM.jpg:Zone.Identifier	3			2020-12-11 17:29:00 EST	2020-12-11 17:29:49 EST	2020-12-11 17:28:59 EST
\$RZFN1Y9L.jpg	2			2020-12-11 17:29:08 EST	2020-12-11 17:29:49 EST	2020-12-11 17:29:06 EST
\$RZFN1Y9L.jpg:Zone.Identifier	3			2020-12-11 17:29:08 EST	2020-12-11 17:29:49 EST	2020-12-11 17:29:06 EST
desktop.ini	7			2018-01-03 01:30:24 EST	2018-01-03 01:30:24 EST	2018-01-03 01:30:24 EST
[current folder]				2020-12-11 18:11:08 EST	2020-12-11 18:11:08 EST	2020-12-11 18:11:08 EST
[parent folder]				2018-01-03 01:30:24 EST	2018-01-03 01:30:24 EST	2018-01-03 01:30:24 EST

File Metadata View:

- Hex
- Text
- Application
- File Metadata
- Context
- Results
- Annotations
- Comments

Annotations View:

- 0°
- 0%
- 74%
- Reset

On analyzing the web searches using Autopsy, Hashbyte has done a lot of searches regarding the murder plan including **how to use the weapons, how to hack CCTV camera, how to brute force the Wi-Fi passwords and about the locations of UTN and Coffee Shop.**

data_1		https://www.bing.com/qbox?query=http%3A%2F%2FutnApartments.com&language=e... 2020-12-11 18:07:42 EST	d
data_1		https://www.bing.com/qbox?query=http%3A%2F%2FutnApartments.co&language=e... 2020-12-11 18:07:42 EST	d
data_1		https://www.bing.com/qbox?query=http%3A%2F%2FutnApartments.co&language=en... 2020-12-11 18:07:41 EST	d
data_1		https://www.bing.com/qbox?query=http%3A%2F%2FutnApartments.&language=en-U... 2020-12-11 18:07:41 EST	d
data_1		https://www.bing.com/qbox?query=http%3A%2F%2FutnApartments.&language=en-U... 2020-12-11 18:07:40 EST	d
data_1		https://www.bing.com/qbox?query=http%3A%2F%2FutnApartments.&language=en-US&pt... 2020-12-11 18:07:40 EST	d
data_1		https://www.bing.com/qbox?query=http%3A%2F%2FutnApartments.&language=en-US&pt=... 2020-12-11 18:07:39 EST	d
data_1		https://www.bing.com/qbox?query=http%3A%2F%2FutnApartments.&language=en-US&pt=Edg... 2020-12-11 18:07:39 EST	d
data_1		https://www.bing.com/qbox?query=http%3A%2F%2FutnApartments.&language=en-US&pt=Edg... 2020-12-11 18:07:36 EST	d
<hr/>			
Hex	Text	Application	File Metadata
Context	Results	Annotations	Other Occurrences
Result: 1... of 1757	Result		
Type	Value		
URL	https://www.bing.com/qbox?query=http%3A%2F%2FutnApartments.&language=en-US&pt=EdgBox&cvid=37ca9f68177d4aae9bb14a61ad5bce2bdd0f1f0&		
Date Created	2020-12-11 18:07:42		
Headers	date : Fri, 11 Dec 2020 20:14:55 GMT content-length : 244 x-msedge-ref : Ref A: 08BE180765AB4540AA371811AEA31347 Ref B: ATAEDGE1020 Ref C: 2020-12-11T20:14:56Z vary : Accept-Encoding content-encoding : br content-type : application/json; charset=utf-8 cache-control : public, max-age=86400 p3p : CP="NON UNI COM NAV STA LOC CURa DEVa PSAa PSDa OUR IND" path : /img_GraduateResearch.E01/Users/IEUser/AppData/Local/Microsoft/Edge/User Data/Default/Cache/data_1/data_1_a00110db path ID : 494982		

data_1		https://www.bing.com/qbox?query=http%3A%2F%2Fccdcoffeeshop.c&language=e... 2020-12-11 18:07:05 ES	
data_1		https://www.bing.com/qbox?query=http%3A%2F%2Fccdcoffeeshop&language=en-US... 2020-12-11 18:07:03 ES	
data_1		https://www.bing.com/qbox?query=http%3A%2F%2Fccdcoffeeshop&language=en-U... 2020-12-11 18:07:03 ES	
data_1		https://www.bing.com/qbox?query=http%3A%2F%2Fccdcoffeeshop&language=en-U... 2020-12-11 18:07:03 ES	
data_1		https://www.bing.com/qbox?query=http%3A%2F%2Fccdcoffees&language=en-US&... 2020-12-11 18:07:02 ES	
data_1		https://www.bing.com/qbox?query=http%3A%2F%2Fccdcoffee&language=en-US&p... 2020-12-11 18:07:01 ES	
data_1		https://www.bing.com/qbox?query=http%3A%2F%2Fccdcoffee&language=en-US&p... 2020-12-11 18:07:01 ES	
data_1		https://www.bing.com/qbox?query=http%3A%2F%2Fccdccoffee&language=en-US&pt=... 2020-12-11 18:06:59 ES	
<hr/>			
Hex	Text	Application	File Metadata
Context	Results	Annotations	Other Occurrences
Result: 179 of 1757	Result		
Type	Value		
URL	https://www.bing.com/qbox?query=http%3A%2F%2Fccdcoffeeshop&language=en-US&pt=EdgBox&cvid=88e99067cc264de9b7b9f94296bc60bcd4&oit		
Date Created	2020-12-11 18:07:03		
Headers	date : Fri, 11 Dec 2020 20:14:12 GMT content-length : 291 x-msedge-ref : Ref A: 49C0B896BE2747FF992895F03F86EFEC Ref B: ATAEDGE1017 Ref C: 2020-12-11T20:14:12Z vary : Accept-Encoding content-encoding : br content-type : application/json; charset=utf-8		

data_1	https://www.bing.com/qbox/?query=&language=en-US&pt=EdgBox&cvid=88e9906/c...	2020-12-11 18:06:52 EST
data_1	http://uncrentals.com/favicon.ico	2020-12-11 18:06:39 EST
data_1	http://uncrentals.com/images/bg.gif	2020-12-11 18:06:38 EST
data_1	http://uncrentals.com/images/blue_bar.gif	2020-12-11 18:06:34 EST
data_1	http://uncrentals.com/images/girlsitting.jpg	2020-12-11 18:06:34 EST
data_1	http://uncrentals.com/images/loading_error.jpg	2020-12-11 18:06:34 EST
data_1	http://uncrentals.com/images/Rental_nav_Front_06.jpg	2020-12-11 18:06:34 EST
data_1	http://uncrentals.com/images/button_bottom_bg.gif	2020-12-11 18:06:34 EST
data_1	http://uncrentals.com/images/Rental_nav_Front_07.jpg	2020-12-11 18:06:34 EST
data_1	http://uncrentals.com/images/Rental_nav_Front_04.jpg	2020-12-11 18:06:34 EST
data_1	http://uncrentals.com/images/Rental_nav_Front_05.jpg	2020-12-11 18:06:34 EST

Hex	Text	Application	File Metadata	Context	Results	Annotations	Other Occurrences
				Result: 667 of 1757	Result		
Type	Value						
URL	http://uncrentals.com/images/bg.gif						
Date Created	2020-12-11 18:06:30						
Headers	date : Fri, 11 Dec 2020 20:13:47 GMT server : Apache last-modified : Fri, 13 Jan 2012 22:14:14 GMT content-length : 809 content-type : image/gif accept-ranges : bytes						
Path	/img_GraduateResearch.E01/Users/IUser/AppData/Local/Microsoft/Edge/User Data/Default/Cache/data_1/data_1_a301103c						
Path ID	493111						
Source File Path	/img_GraduateResearch.E01/Users/IUser/AppData/Local/Microsoft/Edge/User Data/Default/Cache/data_1						
Artifact ID	-9223372036854774470						

data_1	https://d1bk6lwzdwel20.cloudfront.net/script.js	2020-12-11 17:39:29 EST
data_1	https://www.bing.com/images/lbi2mmasvpc=1&ig=FEFD991EDD08764EDDB32D027AC0...	2020-12-11 17:39:26 EST
data_1	https://www.bing.com/qbox/?query=right+point+on+human+body+to+stab+or+kill+...	2020-12-11 17:39:24 EST
data_1	https://www.bing.com/qbox/?query=right+point+on+human+body+to+stab+or+kill+...	2020-12-11 17:39:24 EST
data_1	https://www.bing.com/qbox/?query=right+point+on+human+body+to+stab+or+kill+...	2020-12-11 17:39:24 EST
data_1	https://www.bing.com/qbox/?query=right+point+on+human+body+to+stab+or+kill+...	2020-12-11 17:39:24 EST
data_1	https://www.bing.com/qbox/?query=right+point+on+human+body+to+stab+or+kill+...	2020-12-11 17:39:23 EST
data_1	https://www.bing.com/qbox/?query=right+point+on+human+body+to+stab+or+kill+...	2020-12-11 17:39:23 EST

Hex	Text	Application	File Metadata	Context	Results	Annotations	Other Occurrences
				Result: 154 of 1757	Result		
Type	Value						
URL	https://www.bing.com/qbox/?query=right+point+on+human+body+to+stab+or+kill+using+gun+&language=en-US&pt=EdgBox&9ddaa4f&ig=fe4ae871						
Date Created	2020-12-11 17:39:24						
Headers	date : Fri, 11 Dec 2020 19:42:10 GMT content-length : 140 x-msedge-ref : Ref A: C10021CD9AB649B58DD28916A1AE210C Ref B: ATAEDGE1010 Ref C: 2020-12-11T19:42:10Z vary : Accept-Encoding content-encoding : br content-type : application/json; charset=utf-8 cache-control : public, max-age=86400 p3p : CP="NON UNI COM NAV STA LOC CURa DEVa PSa PSDa OUR IND"						
Path	/img_GraduateResearch.E01/Users/IUser/AppData/Local/Microsoft/Edge/User Data/Default/Cache/data_1/data_1_a0010d73						
Path ID	491693						

	<a href="https://www.bing.com/qbox?query=h&amp;language=en-US&amp;pt=EdgBox&amp;cvid=45c819e4...">https://www.bing.com/qbox?query=h&amp;language=en-US&amp;pt=EdgBox&amp;cvid=45c819e4...</a>	2020-12-11 17:39:03 EST	date : Fri, 11 Dec 2020 19:41:48 GMT
	<a href="https://www.bing.com/images/sbi?mmasync=1&amp;ig=4B1F01DA32DC4F55AE0414592C...">https://www.bing.com/images/sbi?mmasync=1&amp;ig=4B1F01DA32DC4F55AE0414592C...</a>	2020-12-11 17:39:02 EST	date : Fri, 11 Dec 2020 19:41:48 GMT
	<a href="https://www.bing.com/search?q=how+to+hide+evidence&amp;cvid=4e6332bd6214aa3b...">https://www.bing.com/search?q=how+to+hide+evidence&amp;cvid=4e6332bd6214aa3b...</a>	2020-12-11 17:39:01 EST	date : Fri, 11 Dec 2020 19:41:48 GMT
	<a href="https://www.wikihow.com/mobile/images/close.svg">https://www.wikihow.com/mobile/images/close.svg</a>	2020-12-11 17:39:00 EST	date : Fri, 11 Dec 2020 19:41:48 GMT
	<a href="https://www.wikihow.com/load.php?debug=false&amp;lang=en&amp;modules=ext.wikihow.pri...">https://www.wikihow.com/load.php?debug=false&amp;lang=en&amp;modules=ext.wikihow.pri...</a>	2020-12-11 17:39:00 EST	date : Fri, 11 Dec 2020 19:41:48 GMT
	<a href="https://www.wikihow.com/skins/owl/images/nav_messages.optimized.svg">https://www.wikihow.com/skins/owl/images/nav_messages.optimized.svg</a>	2020-12-11 17:39:00 EST	date : Fri, 11 Dec 2020 19:41:48 GMT

Hex | Text | Application | File Metadata | Context | Results | Annotations | Other Occurrences

Result: 278 of 1757 Result ← →

Type	Value
URL	<a href="https://www.bing.com/search?q=how+to+hide+evidence&amp;cvid=4e6332bd6214aa3b...">https://www.bing.com/search?q=how+to+hide+evidence&amp;cvid=4e6332bd6214aa3b...</a>
Date Created	2020-12-11 17:39:01
Headers	date : Fri, 11 Dec 2020 19:41:48 GMT expires : Fri, 11 Dec 2020 19:40:48 GMT nel : {"report_to": "network-errors", "max_age": 604800, "success_fraction": 0.01, "failure_fraction": 1.0} x-msedge-ref : Ref A: 0F490E66F862487B938850AEE5DFF2EE Ref B: ATAEDGE0913 Ref C: 2020-12-11T19:41:48Z vary : Accept-Encoding content-encoding : br link : < <a href="https://r.bing.com">https://r.bing.com</a> >; rel="preconnect"; crossorigin="use-credentials", < <a href="https://r.bing.com">https://r.bing.com</a> >; rel="preconnect"; crossorigin="anonymous" content-type : text/html; charset=utf-8 report-to : {"group": "network-errors", "max_age": 604800, "endpoints": [{"url": "https://aefd.nelreports.net/api/report?cat=bingserp"}]} cache-control : private, max-age=0 p3p : CP="NON UNI COM NAV STA LOC CURA DEVA PSAa PSDa OUR IND"
Path	/img_GraduateResearch.E01/Users/IEUser/AppData/Local/Microsoft/Edge/User Data/Default/Cache/f_000181

	<a href="https://www.wikihow.com/Hide-Evidence-on-a-Computer">https://www.wikihow.com/Hide-Evidence-on-a-Computer</a>	ext.wikihow.ex..
	<a href="https://www.wikihow.com/favicon.ico">https://www.wikihow.com/favicon.ico</a>	
	<a href="https://www.wikihow.com/load.php?debug=false&amp;lang=en&amp;modules=startup&amp;only=s...">https://www.wikihow.com/load.php?debug=false&amp;lang=en&amp;modules=startup&amp;only=s...</a>	
	<a href="https://www.bing.com/th?id=OVP.4m5v1V5qT-4_2zIFpPzNXQEsDh&amp;w=197&amp;h=110&amp;c...">https://www.bing.com/th?id=OVP.4m5v1V5qT-4_2zIFpPzNXQEsDh&amp;w=197&amp;h=110&amp;c...</a>	
	<a href="https://www.bing.com/qbox?query=how+to+hide+eviden&amp;language=en-US&amp;pt=Edg...">https://www.bing.com/qbox?query=how+to+hide+eviden&amp;language=en-US&amp;pt=Edg...</a>	
	<a href="https://www.bing.com/qbox?query=how+to+hide+evidenc&amp;language=en-US&amp;pt=Edg...">https://www.bing.com/qbox?query=how+to+hide+evidenc&amp;language=en-US&amp;pt=Edg...</a>	
	<a href="https://www.bing.com/qbox?query=how+to+hide+evidence&amp;language=en-US&amp;pt=Edg...">https://www.bing.com/qbox?query=how+to+hide+evidence&amp;language=en-US&amp;pt=Edg...</a>	
	<a href="https://www.bing.com/th?id=OVP.S5n2yjLoqdHbNZYJY4NpqQEsDh&amp;w=197&amp;h=110&amp;c...">https://www.bing.com/th?id=OVP.S5n2yjLoqdHbNZYJY4NpqQEsDh&amp;w=197&amp;h=110&amp;c...</a>	

Hex | Text | Application | File Metadata | Context | Results | Annotations | Other Occurrences

Result: 1... of 1757 Result ← →

Type	Value
URL	<a href="https://www.wikihow.com/Hide-Evidence-on-a-Computer">https://www.wikihow.com/Hide-Evidence-on-a-Computer</a>
Date Created	2020-12-11 17:39:00
Headers	date : Fri, 11 Dec 2020 19:41:46 GMT expires : Thu, 01 Jan 1970 00:00:00 GMT vary : Cookie, Accept-Encoding x-frame-options : SAMEORIGIN content-encoding : gzip x-c : cache-wdc5529-WDC,M cache-bwi5147-BWI,m x-content-type-options : nosniff x-xss-protection : 1; mode=block x-timer : S1607715707.651412,VS0,VE129 content-type : text/html; charset=UTF-8 x-p : ma cache-control : private, must-revalidate, max-age=0

data_1	<a href="https://www.bing.com/qbox?query=how+to+use+hydra+for+bruteforce&amp;language=en-US">https://www.bing.com/qbox?query=how+to+use+hydra+for+bruteforce&amp;language=en-US</a>	2020-12-11 17:32:56 EST	access-F
data_1	<a href="https://www.bing.com/qbox?query=how+to+use+hydra+for+bruteforce&amp;language=en-US">https://www.bing.com/qbox?query=how+to+use+hydra+for+bruteforce&amp;language=en-US</a>	2020-12-11 17:32:56 EST	date : F
data_1	<a href="https://www.bing.com/images/search?q=how+to+use+hydra+for+bruteforce&amp;language=en-US">https://www.bing.com/images/search?q=how+to+use+hydra+for+bruteforce&amp;language=en-US</a>	2020-12-11 17:32:56 EST	date : F
data_1	<a href="https://www.bing.com/th?id=OVP.gPcw4EQz5yFL5V9Xo3LnQEsDh&amp;w=197&amp;h=110&amp;c=1">https://www.bing.com/th?id=OVP.gPcw4EQz5yFL5V9Xo3LnQEsDh&amp;w=197&amp;h=110&amp;c=1</a>	2020-12-11 17:32:56 EST	access-F
data_1	<a href="https://www.bing.com/th?id=OVP.ZhIzNxTDMXDRcBcSWNNdAHgFo&amp;w=197&amp;h=110&amp;c=1">https://www.bing.com/th?id=OVP.ZhIzNxTDMXDRcBcSWNNdAHgFo&amp;w=197&amp;h=110&amp;c=1</a>	2020-12-11 17:32:56 EST	access-F
data_1	<a href="https://pagead2.googlesyndication.com/pcs/activeview?xai=AKAOjstJN8j1-PQxFGHJc...">https://pagead2.googlesyndication.com/pcs/activeview?xai=AKAOjstJN8j1-PQxFGHJc...</a>	2020-12-11 17:32:56 EST	date : F
data_1	<a href="https://pagead2.googlesyndication.com/pcs/activeview?xai=AKAOjst9uofhzsMTpTZjh...">https://pagead2.googlesyndication.com/pcs/activeview?xai=AKAOjst9uofhzsMTpTZjh...</a>	2020-12-11 17:32:56 EST	date : F
data_1	<a href="https://www.bing.com/th?id=OVP.CsJdV6tUx6vmY1RawZxEvAEsDh:OVP.yJjxO8cSQ...">https://www.bing.com/th?id=OVP.CsJdV6tUx6vmY1RawZxEvAEsDh:OVP.yJjxO8cSQ...</a>	2020-12-11 17:32:56 EST	access-F
data_1	<a href="https://www.bing.com/qbox?query=how+to+use+hydra+for+brute&amp;language=en-US">https://www.bing.com/qbox?query=how+to+use+hydra+for+brute&amp;language=en-US</a>	2020-12-11 17:32:55 EST	date : F
data_1	<a href="https://www.bing.com/qbox?query=how+to+use+hydra+for+brutefor&amp;language=en-US">https://www.bing.com/qbox?query=how+to+use+hydra+for+brutefor&amp;language=en-US</a>	2020-12-11 17:32:55 EST	date : F

data_1	https://snap.lcdn.com/li.lms-analytics/insight.beta.min.js	2020-12-11 17:32:33 EST	date : Fri, 11 Dec 2020	
data_1	https://assets.ubembed.com/universalscript/releases/v0.178.1/bundle.js	2020-12-11 17:32:33 EST	date : Sun, 11 Oct 2020	
data_1	https://www.bing.com/search?q=how+to+bruteforce+ wifi+passwords&cvid=816168... 2020-12-11 17:32:33 EST	2020-12-11 17:32:33 EST	date : Fri, 11 Dec 2020	
data_1	https://www.google-analytics.com/gtm.js?id=GTM-3M9H7&f=gaq_GA_F40309_0&t=... 2020-12-11 17:32:33 EST	2020-12-11 17:32:33 EST	date : Fri, 11 Dec 2020	
data_1	https://a.omappapi.com/app/js/webfont/1.5.18/webfont.js	2020-12-11 17:32:33 EST	date : Fri, 11 Dec 2020	
data_1	https://script.hotjar.com/modules.9dd23155c7d4a9746d0b.js	2020-12-11 17:32:33 EST	date : Fri, 11 Dec 2020	
data_1	https://resources.infosecinstitute.com/wp-content/themes/infores/images/logo@2x.png	2020-12-11 17:32:33 EST	date : Fri, 11 Dec 2020	
data_1	https://c.disquscdn.com/next/embed/styles/lounge.2a0be1cac62547aa91037395a06... 2020-12-11 17:32:33 EST	2020-12-11 17:32:33 EST	date : Fri, 11 Dec 2020	
data_1	https://a.omappapi.com/users/6ff8e07f7e29/images/a4c94e5c5fe31605310542-Infos... 2020-12-11 17:32:33 EST	2020-12-11 17:32:33 EST	date : Fri, 11 Dec 2020	
data_1	https://secure.gravatar.com/avatar/e4dc3c6c7fe7831e35d9354acf535b46?s=50&d=... 2020-12-11 17:32:33 EST	2020-12-11 17:32:33 EST	date : Fri, 11 Dec 2020	
data_1	https://c.disquscdn.com/next/embed/lounge.load.71959148e30df0c2d536c080e2d8c... 2020-12-11 17:32:33 EST	2020-12-11 17:32:33 EST	date : Fri, 11 Dec 2020	

Password cracking tools like **Hydra** and **Johnny (John the Ripper)** were also downloaded and installed and were found in the “Downloads” Folder in the location

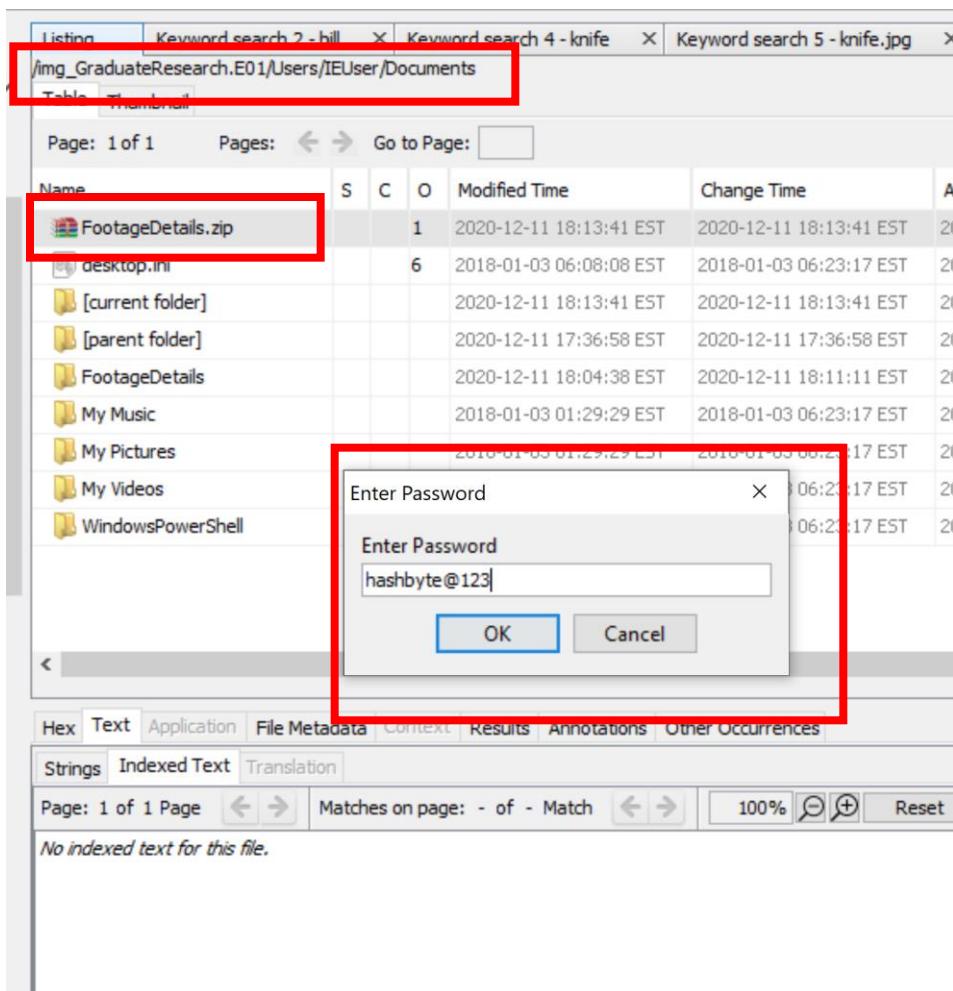
/img\_GraduateResearch.E01/Users/IEUser/Downloads.

The screenshot shows a Windows File Explorer window on the left and a forensic analysis tool interface on the right. The File Explorer shows a tree view of the 'Downloads' folder, which contains several files and sub-folders. A red box highlights the 'Downloads' folder. The forensic tool interface shows a table of files from the '/img\_GraduateResearch.E01/Users/IEUser/Downloads' directory. A red box highlights four specific files: 'Hydra-GUI-master.zip', 'Hydra-GUI-master.zip:Zone.Identifier', 'johnny\_2.2\_win.zip', and 'johnny\_2.2\_win.zip:Zone.Identifier'. Below the table, a detailed view of 'Hydra-GUI-master.zip' is shown, including its name, type (File System), MIME type (application/zip), and size (342897).

Name	Type	MIME Type	Size
/img_GraduateResearch.E01/Users/IEUser/Downloads/Hydra-GUI-master.zip	File System	application/zip	342897

In the “Documents” folders, there was a password zipped file named “**FootageDetails.zip**”. I cracked the password of the zip file using **fcrackzip v1.0** tool in my Kali Linux and found the password to be **hashbyte@123**

```
root@kali:~          root@kali: ~/Desktop 168x32
# fcrackzip -u -D -p commonpassword.txt FootageDetails.zip
PASSWORD FOUND!!!!: pw == hashbyte@123
#
```



In the FootageDetails folder, there were pictures of **CCTV footages** and **Hydra** where the target was set to be <http://ccdcoffeeshop.com> to brute force the Wi-Fi password of the coffee shop using Hydra tool.

The image shows two windows side-by-side. The left window is a file explorer with a red box around the address bar showing the path: /Img\_GraduateResearch.E01/Users/IEUser/Documents/FootageDetails. It lists several files including 'Hydra.PNG'. The right window is the THC Hydra GUI v0.2 - Xyl0k (White Hat Edition) with a red box around the 'Target' field containing 'http://ccdcoffeeshop.com'.

Page: 1 of 1 Pages: < > Go to Page: [ ]

Name	S	C	O	Modified Time	Change Time	Access T
wifipassword.txt				1 2020-12-11 18:13:01 EST	2020-12-11 18:13:01 EST	2020-12-
<b>Hydra.PNG</b>				1 2020-12-11 17:35:31 EST	2020-12-11 18:04:19 EST	2020-12-
cctv footage 1.jpg:Zone.Identifier				2 2020-12-11 17:29:06 EST	2020-12-11 18:04:38 EST	2020-12-
cctv footage 2 (1).jpg				2 2020-12-11 17:28:56 EST	2020-12-11 18:04:38 EST	2020-12-
cctv footage 2 (1).jpg:Zone.Identifier				3 2020-12-11 17:28:56 EST	2020-12-11 18:04:38 EST	2020-12-
cctv footage 4.ico				2 2020-12-11 17:29:10 EST	2020-12-11 18:04:38 EST	2020-12-

Hex Text Application File Metadata Context Results Annotations Other Occurrences

0° C C 38% 🔎 ⚖️ Reset

THC Hydra GUI v0.2 - Xyl0k (White Hat Edition)

Protocol

- HTML Auth
- HTTP Auth
- RDP
- FTP

Login authentication

User:  Single: admin  
 Wordlist

Charset

abcdefghijklmnopqrstuvwxyz0123456789

Min: 1

Max: 9

Options

Show login+pass combination for each attempt

Loop around users, not passwords

Exit when a login/pass pair is found

Write found login/password pairs to result.txt

Waittime for responses 64

Login as pass

HTTP Configuration

Target:  ?

Port:  ?

Name	S	C	O	Modified Time	Change Time	Access Time	Created Ti
wifipassword.txt				1 2020-12-11 18:13:01 EST	2020-12-11 18:13:01 EST	2020-12-11 18:03:57 EST	2020-12-11
cctv footage 1.jpg				1 2020-12-11 17:35:31 EST	2020-12-11 18:04:19 EST	2020-12-11 17:35:31 EST	2020-12-11
cctv footage 1.jpg				2 2020-12-11 17:29:06 EST	2020-12-11 18:04:38 EST	2020-12-11 17:29:04 EST	2020-12-11
cctv footage 2 (1).jpg				3 2020-12-11 17:29:06 EST	2020-12-11 18:04:38 EST	2020-12-11 17:29:04 EST	2020-12-11
cctv footage 2 (1).jpg:Zone.Identifier				2 2020-12-11 17:28:56 EST	2020-12-11 18:04:38 EST	2020-12-11 17:28:55 EST	2020-12-11
cctv footage 4.ico				3 2020-12-11 17:28:56 EST	2020-12-11 18:04:38 EST	2020-12-11 17:28:55 EST	2020-12-11
				2 2020-12-11 17:29:10 EST	2020-12-11 18:04:38 EST	2020-12-11 17:29:08 EST	2020-12-11

Hex Text Application File Metadata Context Results Advanced Options Other Options

0° C C 86% 🔍 ⌂ | Reset



There was also a .txt file named “**wifipassword.txt**” in which CCD Coffee shop Wi-Fi credentials of admin were stored and the **password was stored in MD5 hash**.

The screenshot shows a file analysis interface. At the top, there is a file list table with columns: NAME, S, C, O, Modified Time, Change Time, and Ac. A red box highlights the row for 'wifipassword.txt'. Below the table is a text viewer with tabs: Hex, Text, Application, File Metadata, Context, Results, Annotations, Other Occurrences, Strings, Indexed Text, and Translation. The 'Text' tab is selected. A red box highlights the text content, which reads:

```
CCD Coffee shop wifi credentials
username : admin
password: 5d896cd278363908292d1fde8315c1b8
```

Below the text viewer is a footer bar with buttons for Page navigation, search, and zoom.

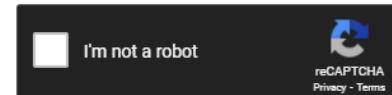
I was able to **crack the original value of the hash using an online tool – Crack Station**.

And found the password to be **coffee123**

## Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

5d896cd278363908292d1fde8315c1b8



## Crack Hashes

 reCAPTCHA  
Privacy - Terms

**Supports:** LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (`sha1(sh1_bin)`)  
QubesV3.1BackupDefaults

Hash	Type	Result
5d896cd278363908292d1fdfe8315c1b8	md5	coffee123

**Color Codes:** Green: Exact match, Yellow: Partial match, Red: Not found

On analyzing the Prefetch folder using **WinPrefetchView tool**, I was able to find the most run programs to be **HYDRAGUI.EXE** and **JOHNNY.EXE**

Finally, a **murder image** was also found in the Recycle Bin Folder.

/img\_GraduateResearch.E01/\$Recycle.Bin/S-1-5-21-3040204872-3082932231-1584796067-1001

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
\$IMN5089.jpg		1		2020-12-11 17:29:49 EST	2020-12-11 17:29:49 EST	2020-12-11 17:29:49 EST	2020-12-11 17:29:49
\$IQ7Y9ZM.jpg		1		2020-12-11 17:29:49 EST	2020-12-11 17:29:49 EST	2020-12-11 17:29:49 EST	2020-12-11 17:29:49
\$1ZFN9L.jpg		1		2020-12-11 17:29:49 EST	2020-12-11 17:29:49 EST	2020-12-11 17:29:49 EST	2020-12-11 17:29:49
<b>\$R6GR0VM.jpg</b>		1		2020-12-11 17:29:14 EST	2020-12-11 17:30:34 EST	2020-12-11 17:29:13 EST	2020-12-11 17:29:13
\$R6GR0VM.jpg:Zone.Identifier		3		2020-12-11 17:29:14 EST	2020-12-11 17:30:34 EST	2020-12-11 17:29:13 EST	2020-12-11 17:29:13
\$R8W04JP.jpg		2		2020-12-11 17:29:16 EST	2020-12-11 17:31:20 EST	2020-12-11 17:29:15 EST	2020-12-11 17:29:15
\$R8W04JP.tbo:Zone.Identifier		3		2020-12-11 17:29:16 EST	2020-12-11 17:31:20 EST	2020-12-11 17:29:15 EST	2020-12-11 17:29:15

Hex Text Application File Metadata Context Results Annotations Other Occurrences

0° C C 234% ⌂ ⌂ Reset



Analvzino files from GraduateResearch.E01

## Conclusion

After acquiring the image file (GraduateResearch.E01) stated above, I performed many processes as part of forensic examination to analyze the lab in detail using FTK Imager and Autopsy. Using Autopsy, I was able to identify email communications between two users, identify the email addresses of those users, locate the pictures of murder weapons, cracked the password zipped file using fcrackzip, cracked hashed passwords using CrackStation and the most run programs using WinPrefetchView tool. Also, finally I used FTK Imager to verify the given images to ensure no data was tampered during the analysis phase.

## **GraduateResearch.E01**

Drive/Image Verify Results	
Sector count	46077952
MD5 Hash	
Computed hash	4938212c1126f6c8e7052964b2e4197c
Stored verification hash	4938212c1126f6c8e7052964b2e4197c
Report Hash	4938212c1126f6c8e7052964b2e4197c
Verify result	Match
SHA1 Hash	
Computed hash	4adb6bb55eaede4f9a47bcd0032a683b0cf0
Stored verification hash	4adb6bb55eaede4f9a47bcd0032a683b0cf0
Report Hash	4adb6bb55eaede4f9a47bcd0032a683b0cf0
Verify result	Match
Bad Blocks List	
Bad blocks in image	No bad blocks found in image
Close	

Signed:

Vinitha Mathiyazhagan

---

DFE Vinitha Mathiyazhagan

Digital Forensics Examiner

UNCC Forensics Lab