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.

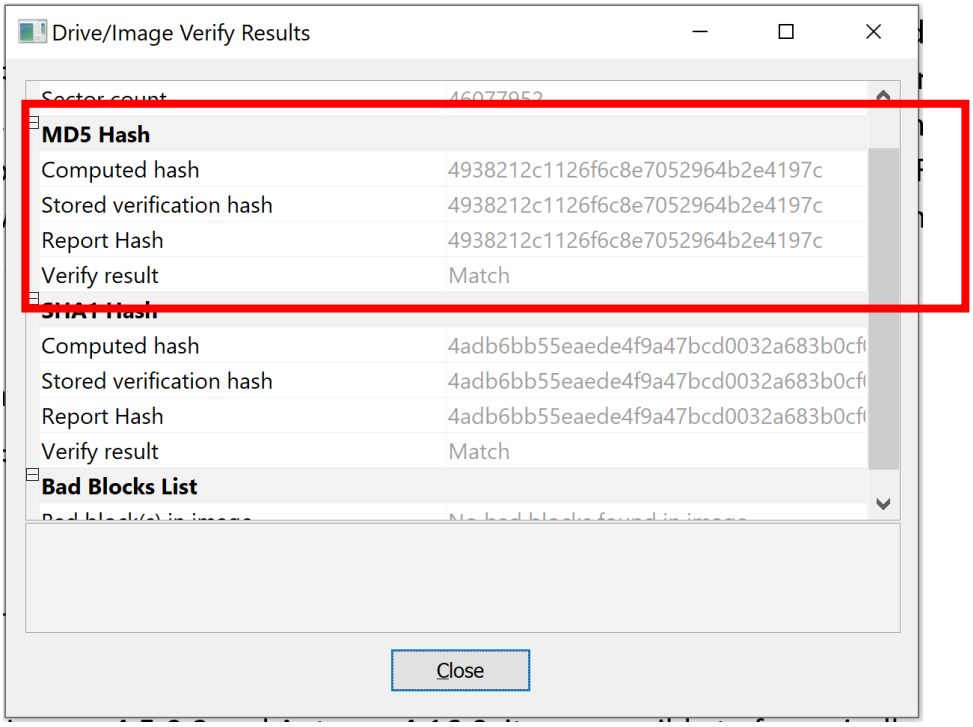
Kali Linux was also used to crack the password for zipped folder using fcrackzip and an online tool **Crack Station** was used to find the original value of the hashes found.

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:

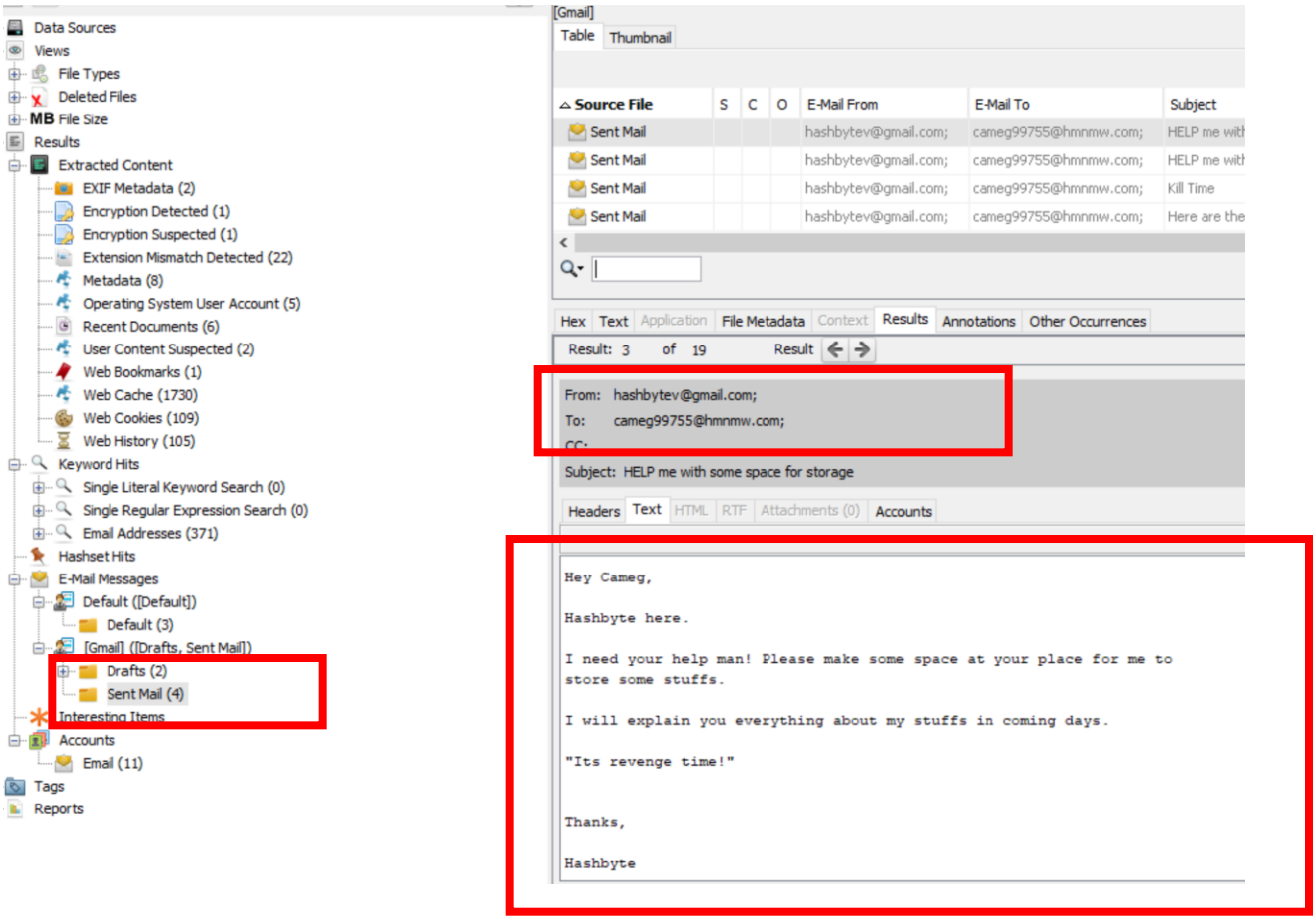
GraduateResearch.E01



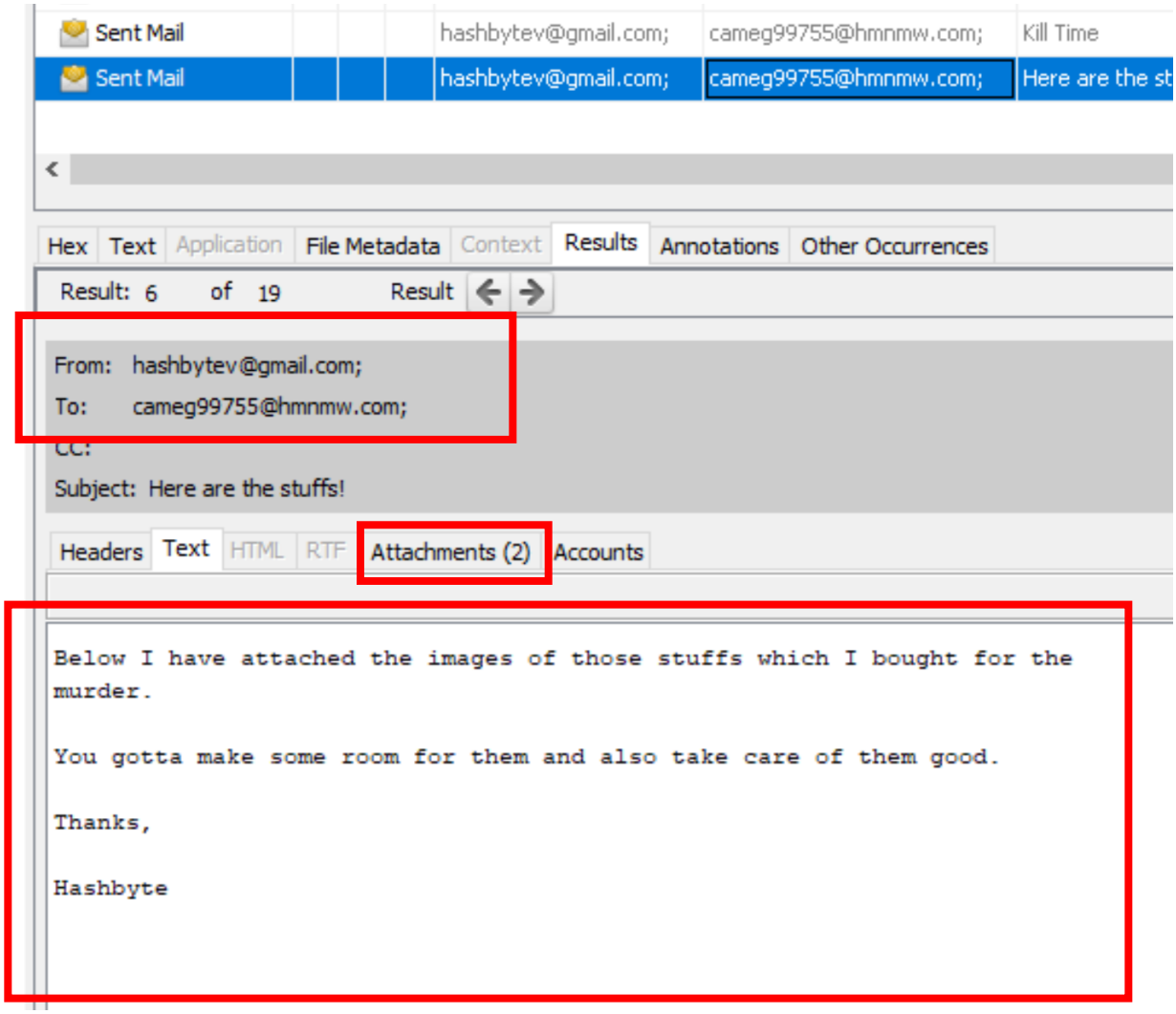
Findings and Report (Forensic Analysis)

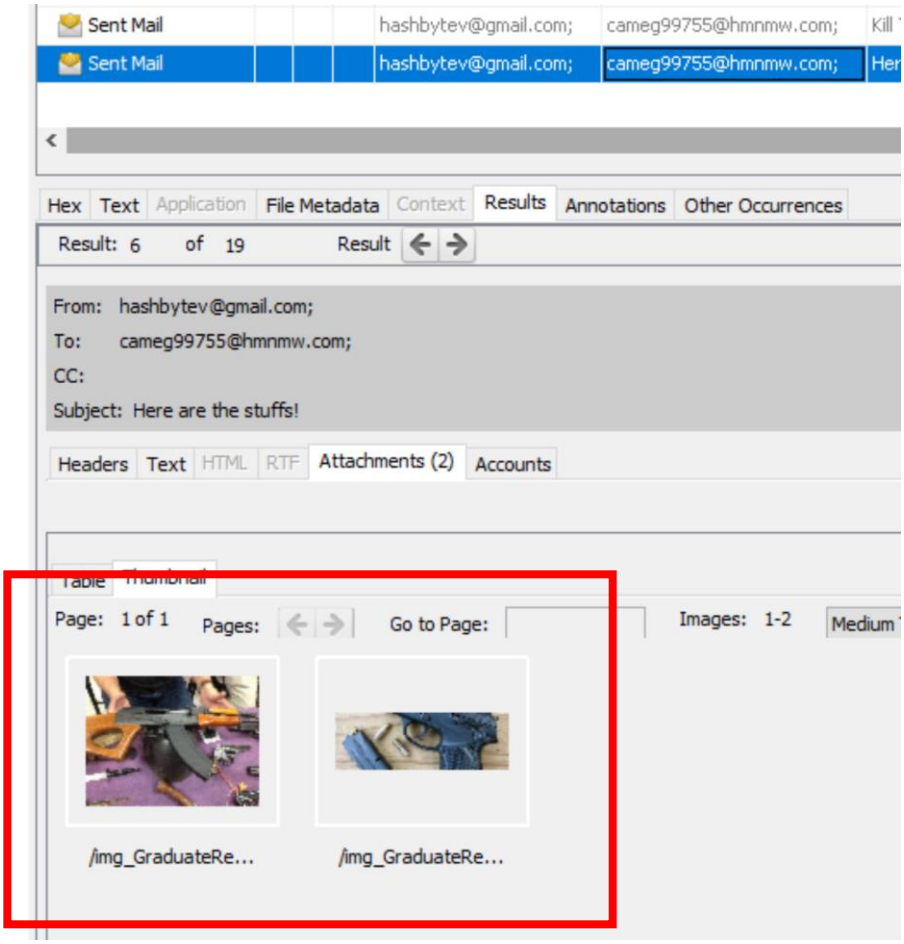
Using FTK Imager 4.5.0.3 and Autopsy 4.16.0, it was possible to forensically analyze the image in detail. Each item is addressed separately below.

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



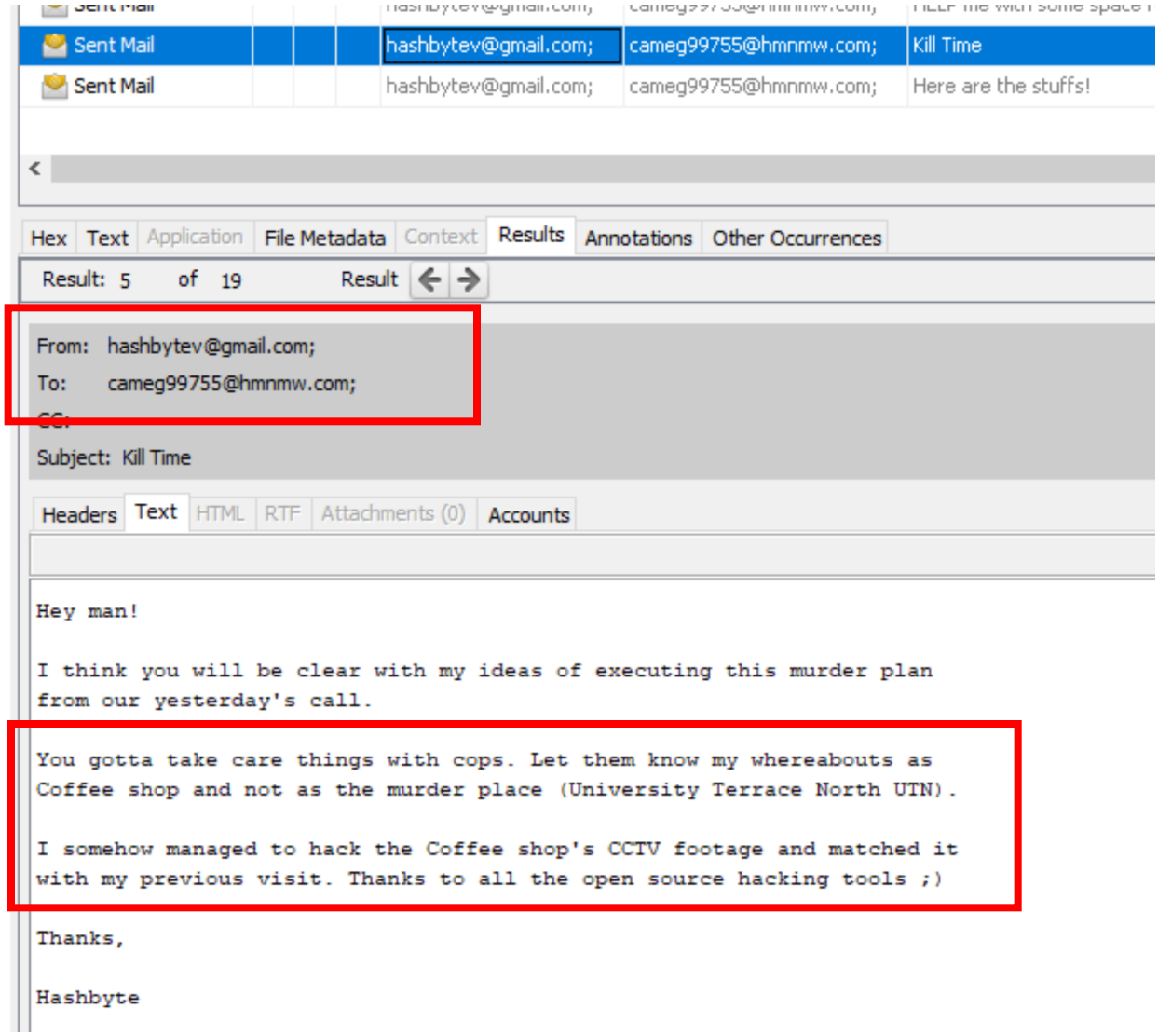
There were also few images attached to an email explaining about **his stuffs for identification**.



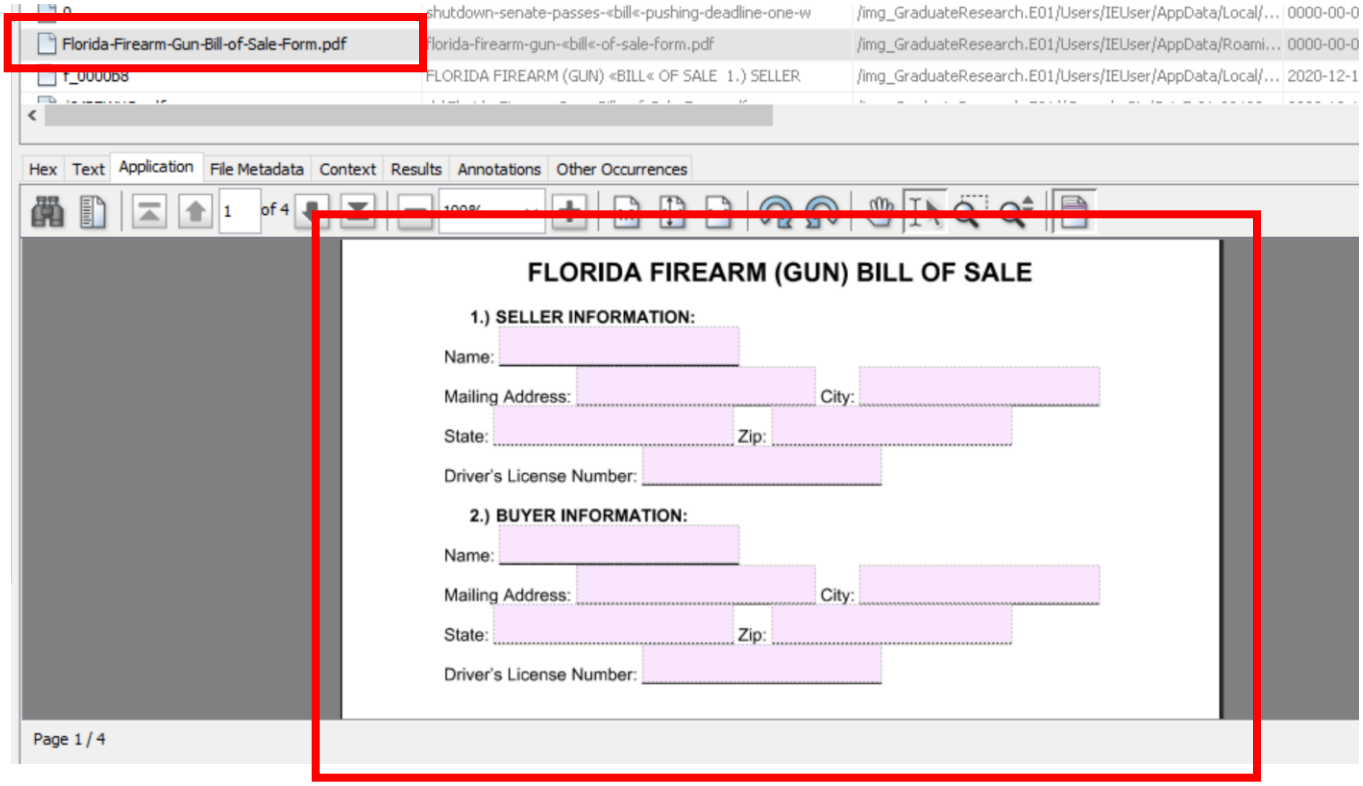

Sent Mail
hashbytev@gmail.com;
cameg99755@hmnmw.com;
Sent Mail
hashbytev@gmail.com;
cameg99755@hmnmw.com;
Hex
Text
Application
File Metadata
Context
Results
Annotations
Other Occurrences
Result: 6 of 19
Result
From: hashbytev@gmail.com;
To: cameg99755@hmnmw.com;
CC:
Subject: Here are the stuffs!
Headers
Text
HTML
RTF
Attachments (2)
Accounts
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.

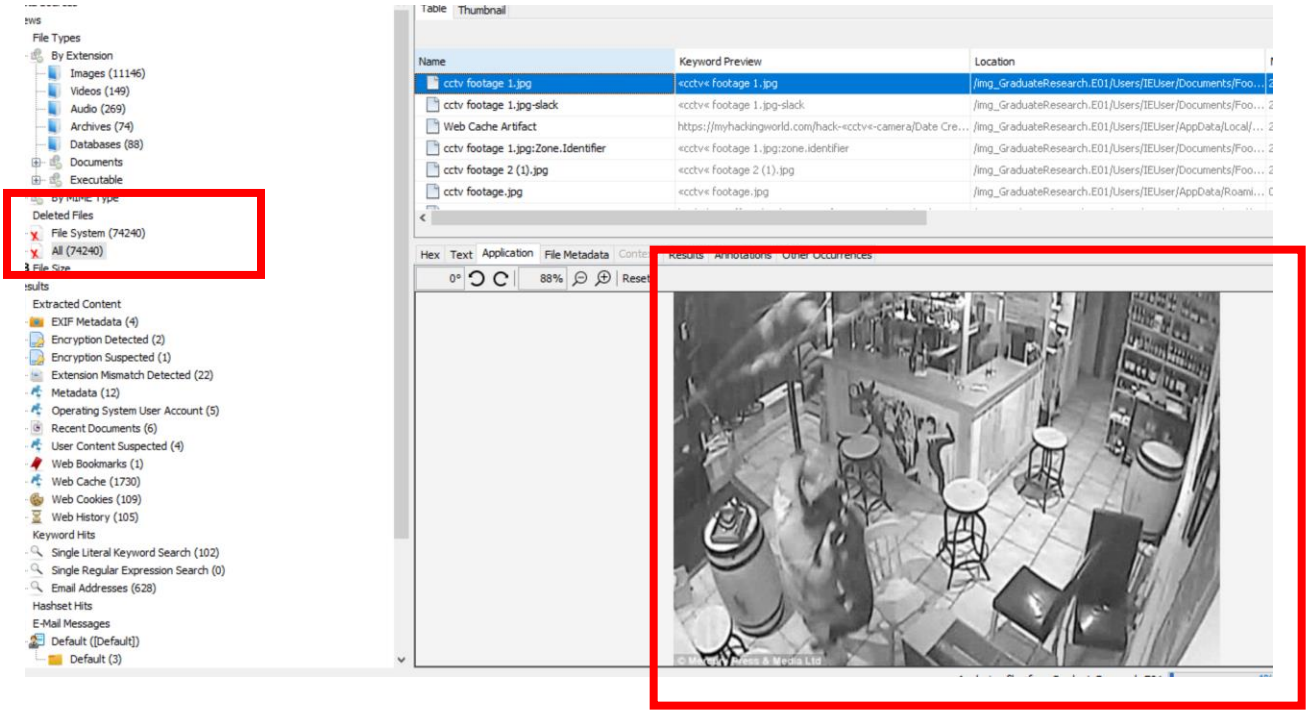
And he was also successful in hacking the **wifi password** and the **CCTV footage of the Coffee Shop** to place his earlier visit picture as a footage during the murder time as per his email communication.

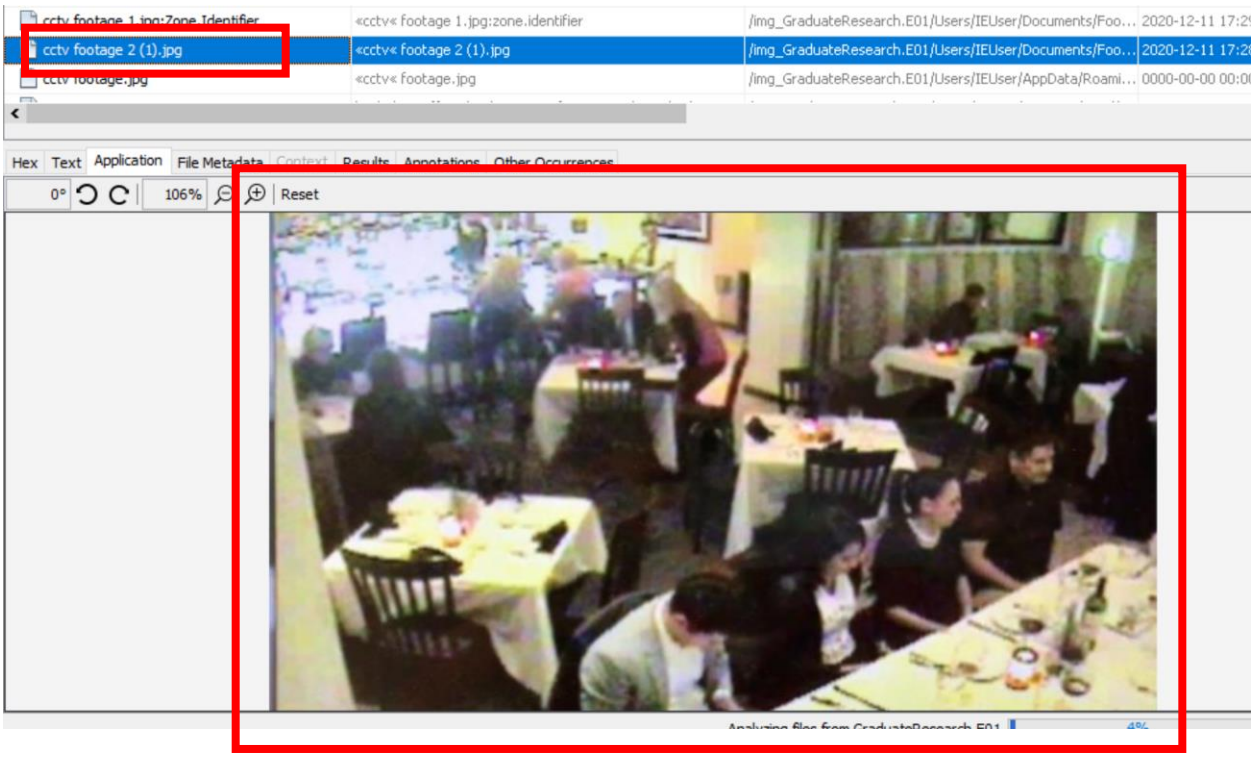


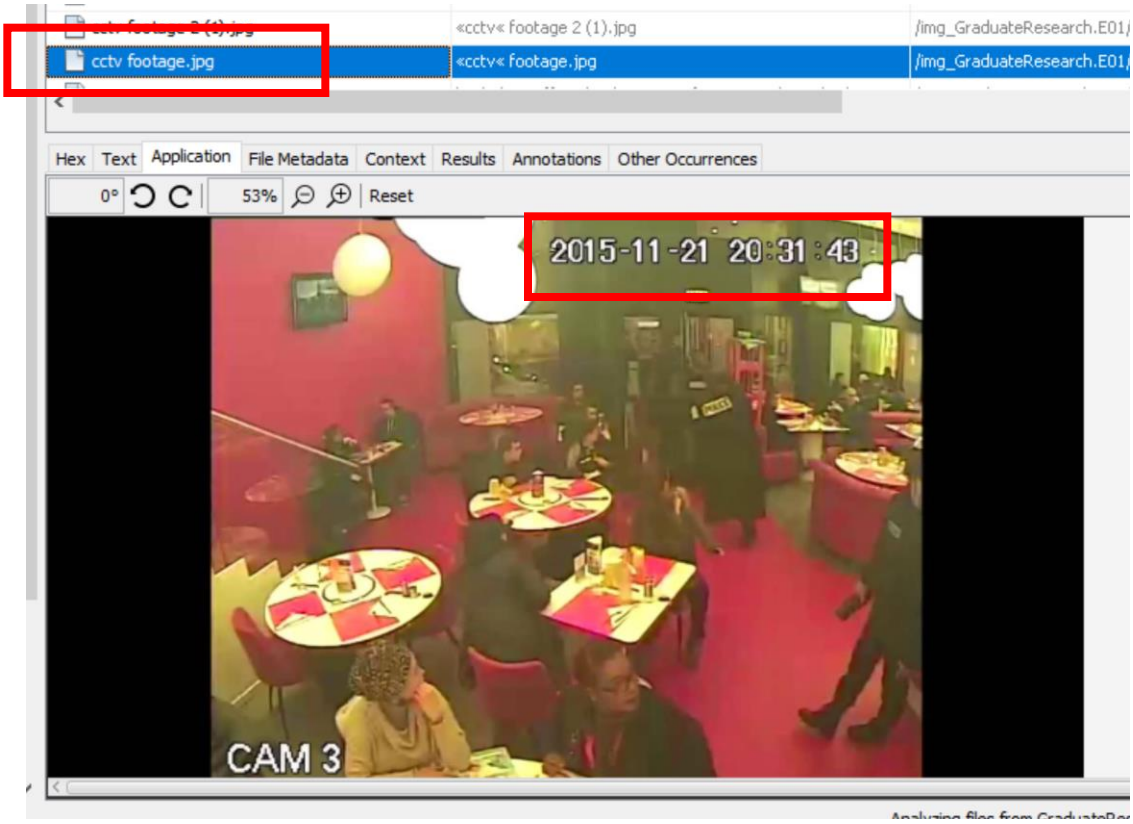
In **the "Deleted Folder",** there was a **FLORIDA FIREARM (GUN) BILL OF SALE** pdf file which might have been filled up by Hashbyte to buy a gun.

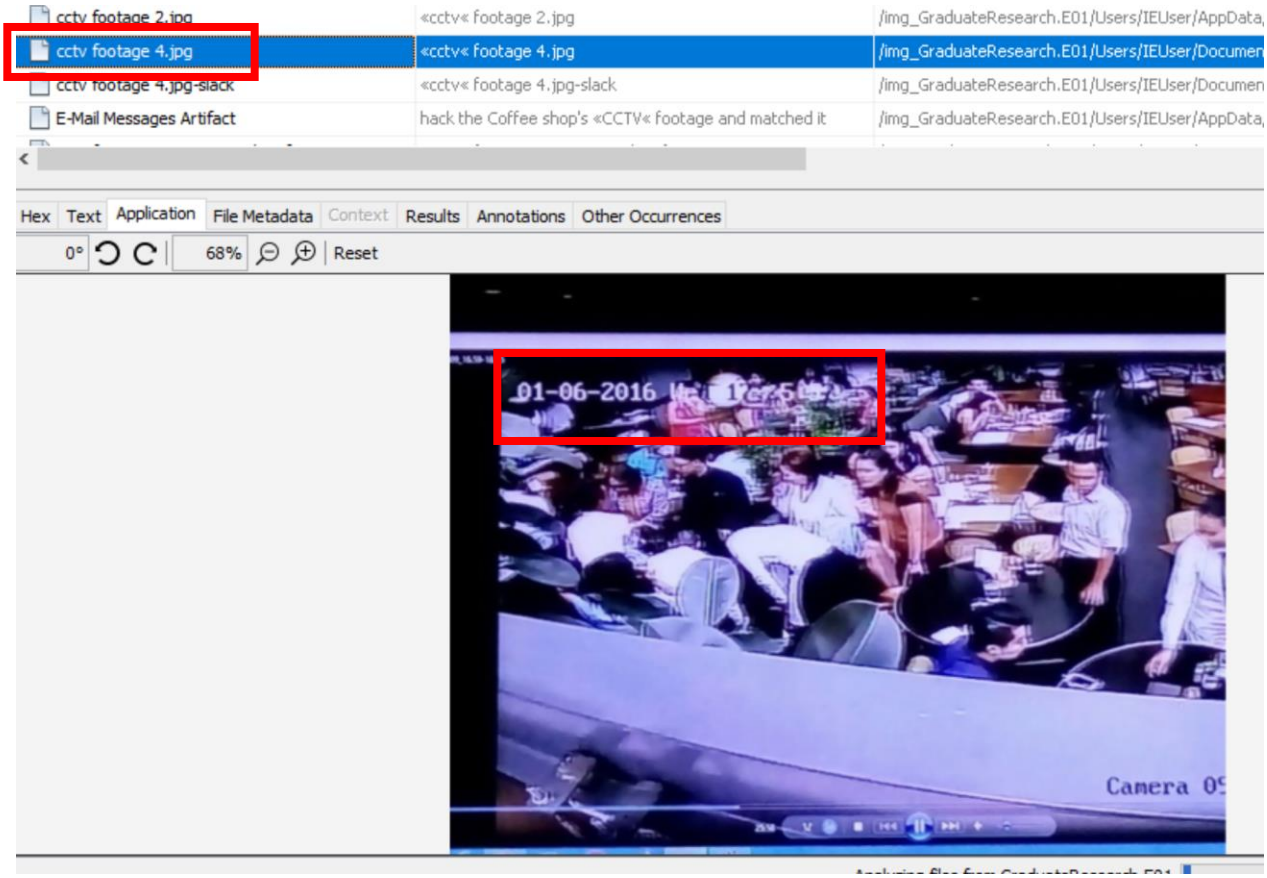


There was also some CCTV footage in the **"Deleted Folder", gun and rifle pictures in "Downloads"** were found using Autopsy.




cctv footage 1.jpg:Zone.Identifier
«cctv« footage 1.jpg:zone.identifier
/img_GraduateResearch.E01/Users/IEUser/Documents/Foo...
2020-12-11 17:2
cctv footage 2 (1).jpg
«cctv« footage 2 (1).jpg
/img_GraduateResearch.E01/Users/IEUser/Documents/Foo...
2020-12-11 17:2
«cctv« footage.jpg
/img_GraduateResearch.E01/Users/IEUser/AppData/Roami...
0000-00-00 00:0
Hex
Text
Application
File Metadata
Context
Results
Annotations
Other Occurrences
0°
106%
Reset

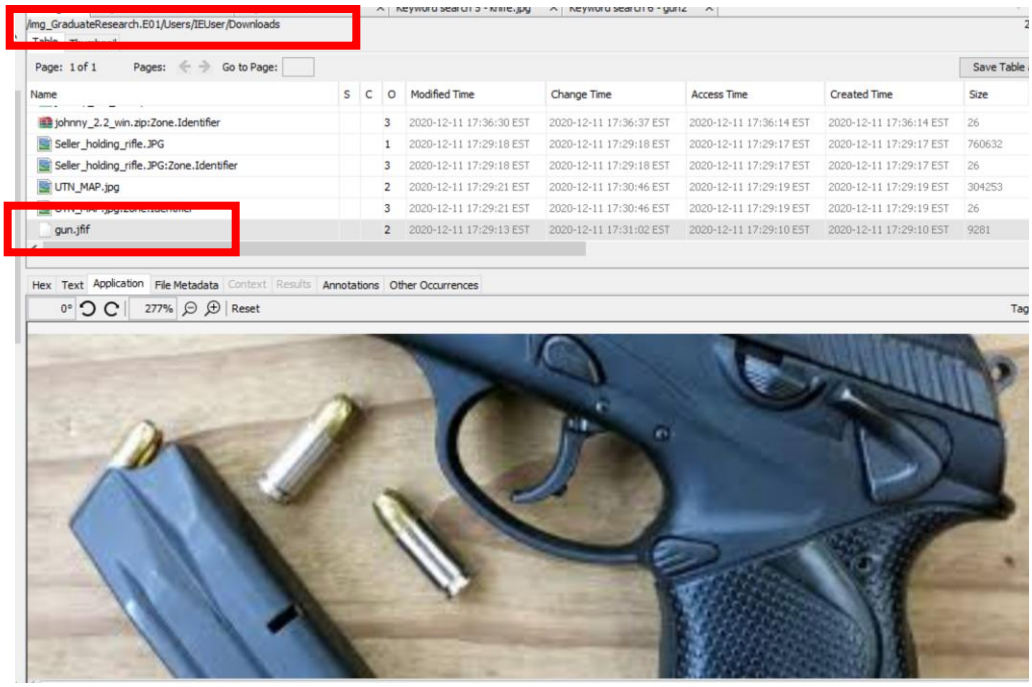

«cctv« footage 2 (1).jpg
/img_GraduateResearch.E01/
cctv footage.jpg
«cctv« footage.jpg
/img_GraduateResearch.E01/
Hex
Text
Application
File Metadata
Context
Results
Annotations
Other Occurrences
0°
53%
Reset
2015-11-21 20:31:43
CAM 3

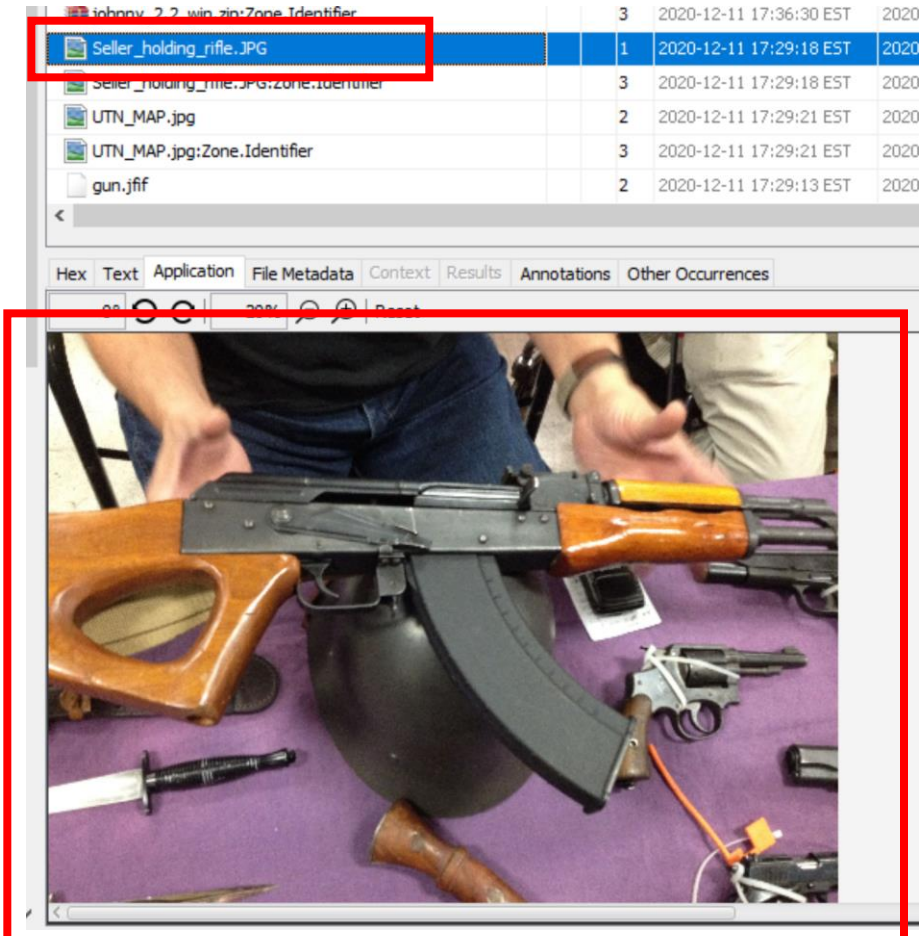


The above date captured in the footage (which is a lot earlier) **does not match** with the recent murder date happened as per the statement provided.

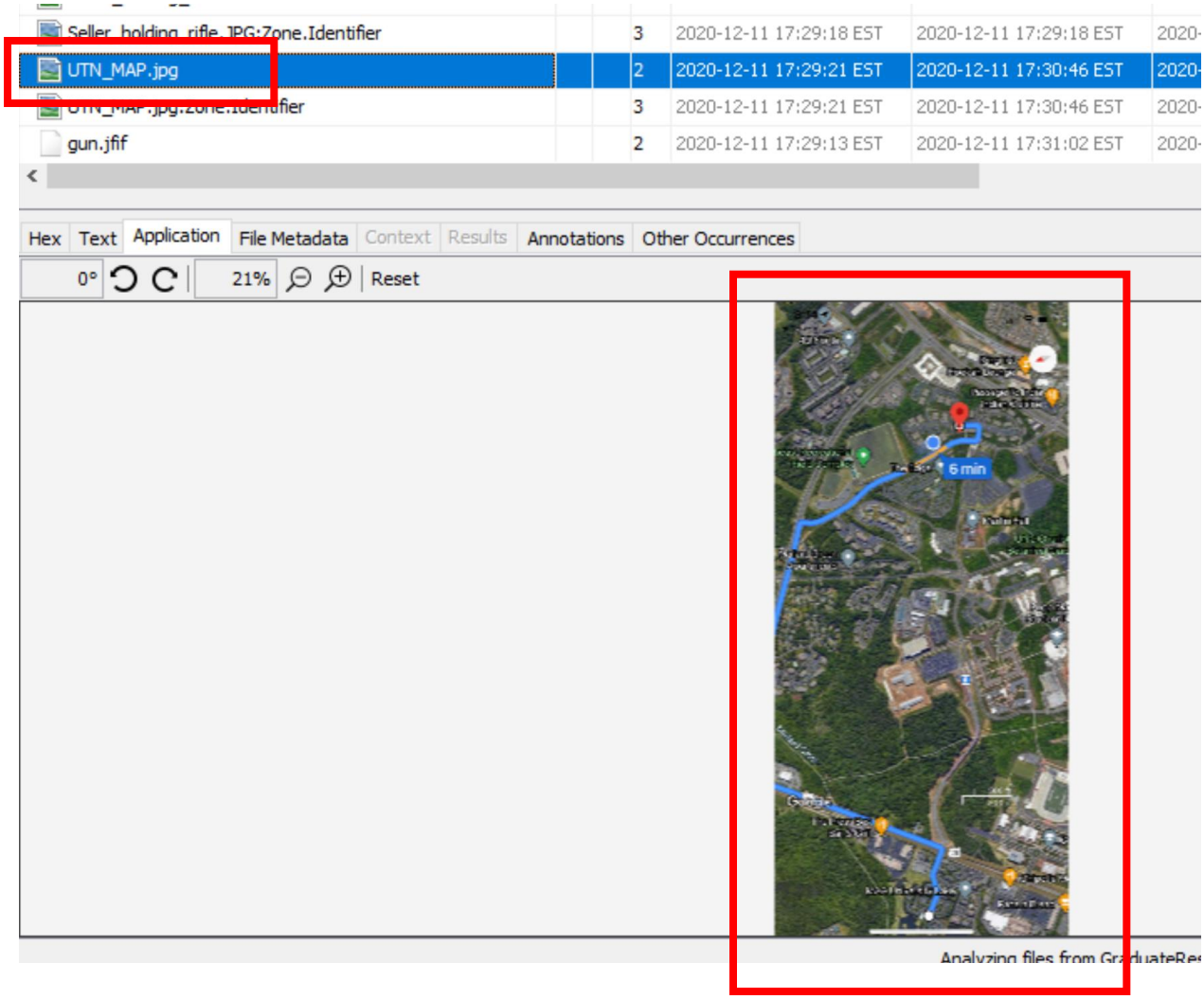
Images of Gun and Rifle in the location

/img_GraduateResearch.E01/Users/IEUser/Downloads/


/img_GraduateResearch.E01/Users/IEUser/Downloads
Page: 1 of 1
Pages:
Go to Page:
Save Table
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
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
277%
Reset

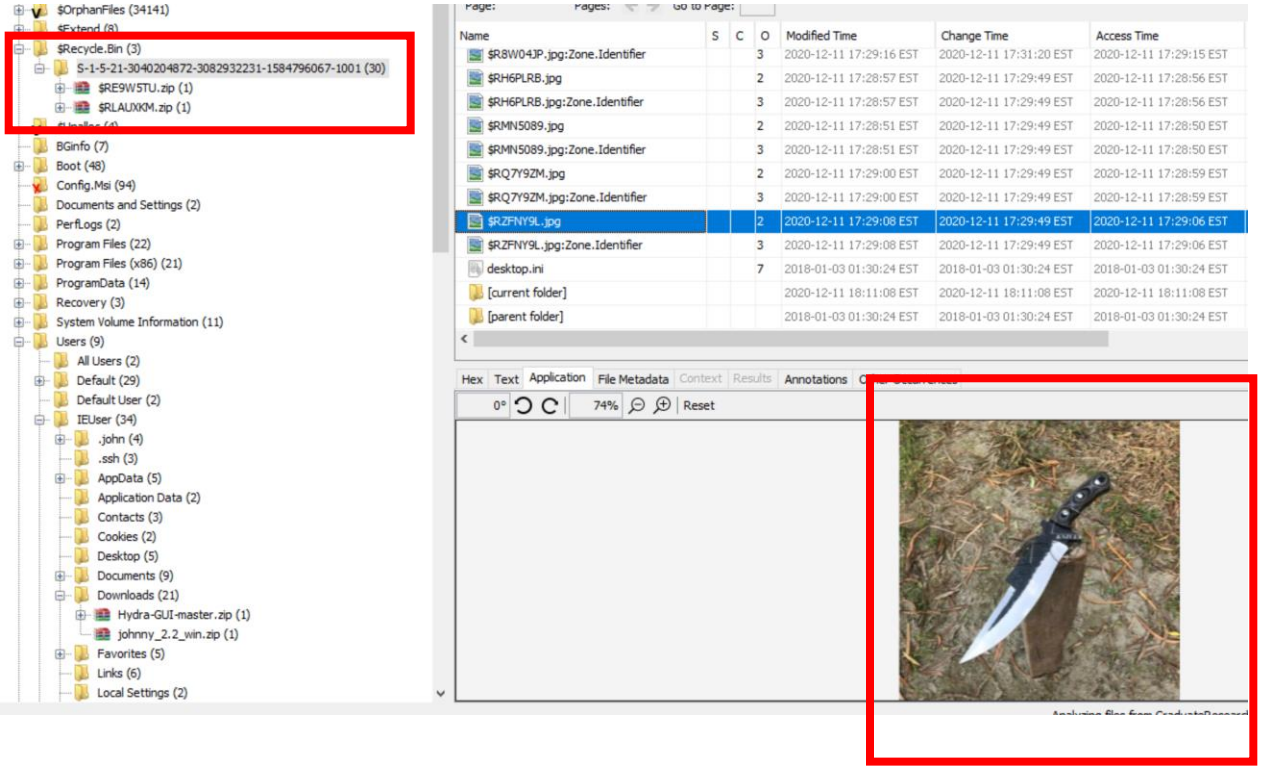

johnny_2.2_win.zip:Zone.Identifier 3 2020-12-11 17:36:30 EST 2020
Seller_holding_rifle.JPG 1 2020-12-11 17:29:18 EST 2020
3 2020-12-11 17:29:18 EST 2020
UTN_MAP.jpg 2 2020-12-11 17:29:21 EST 2020
UTN_MAP.jpg:Zone.Identifier 3 2020-12-11 17:29:21 EST 2020
gun.jfif 2 2020-12-11 17:29:13 EST 2020
Hex
Text
Application
File Metadata
Context
Results
Annotations
Other Occurrences
Reset

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.

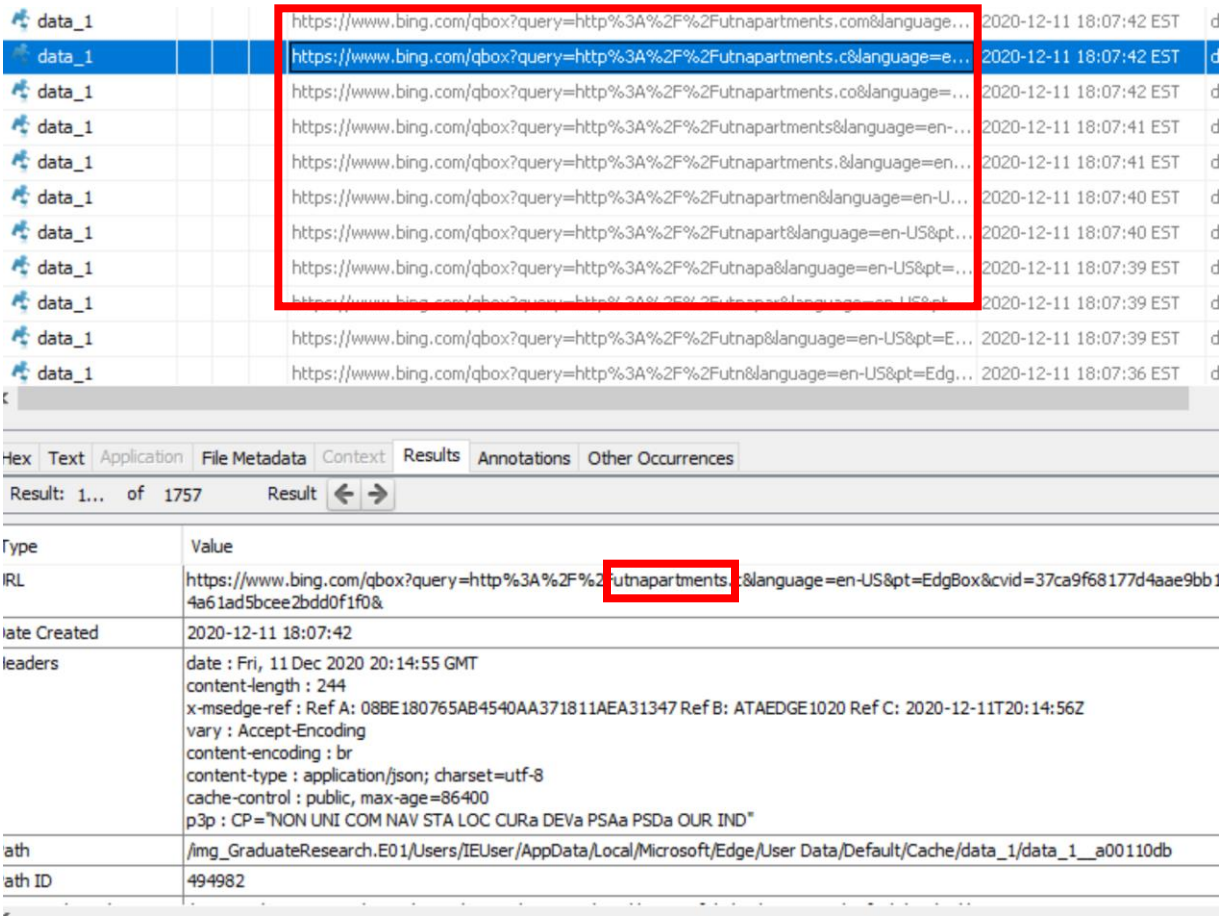


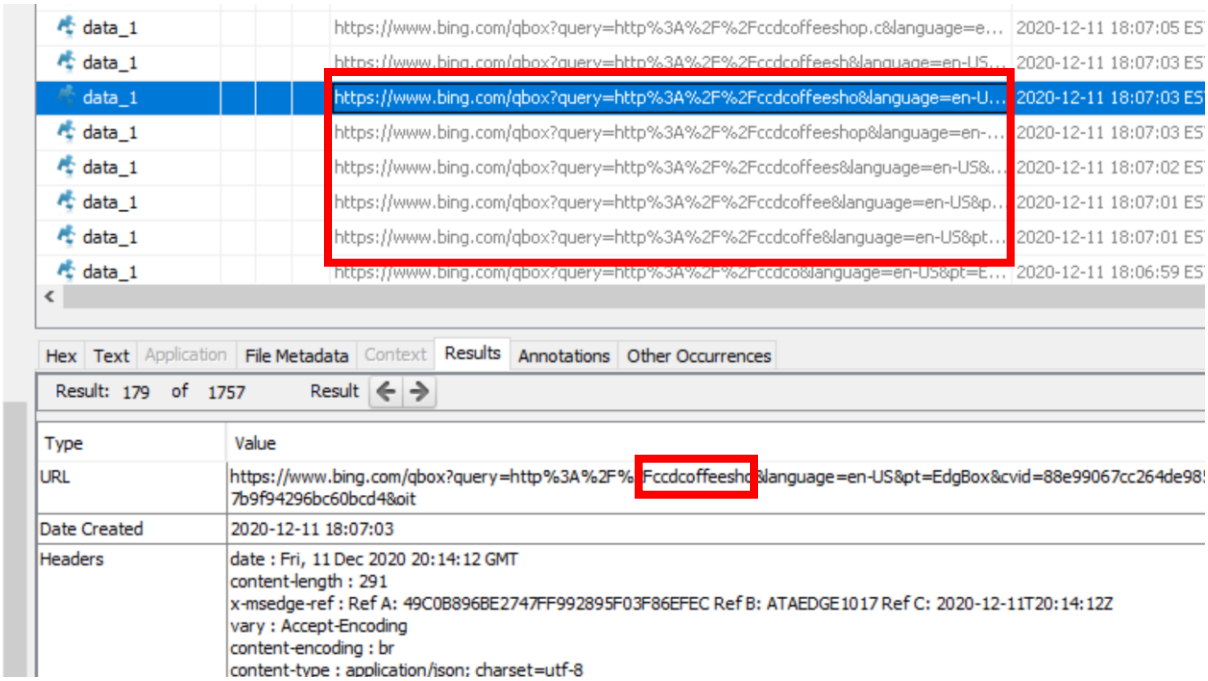
An image of knife was also found in the location

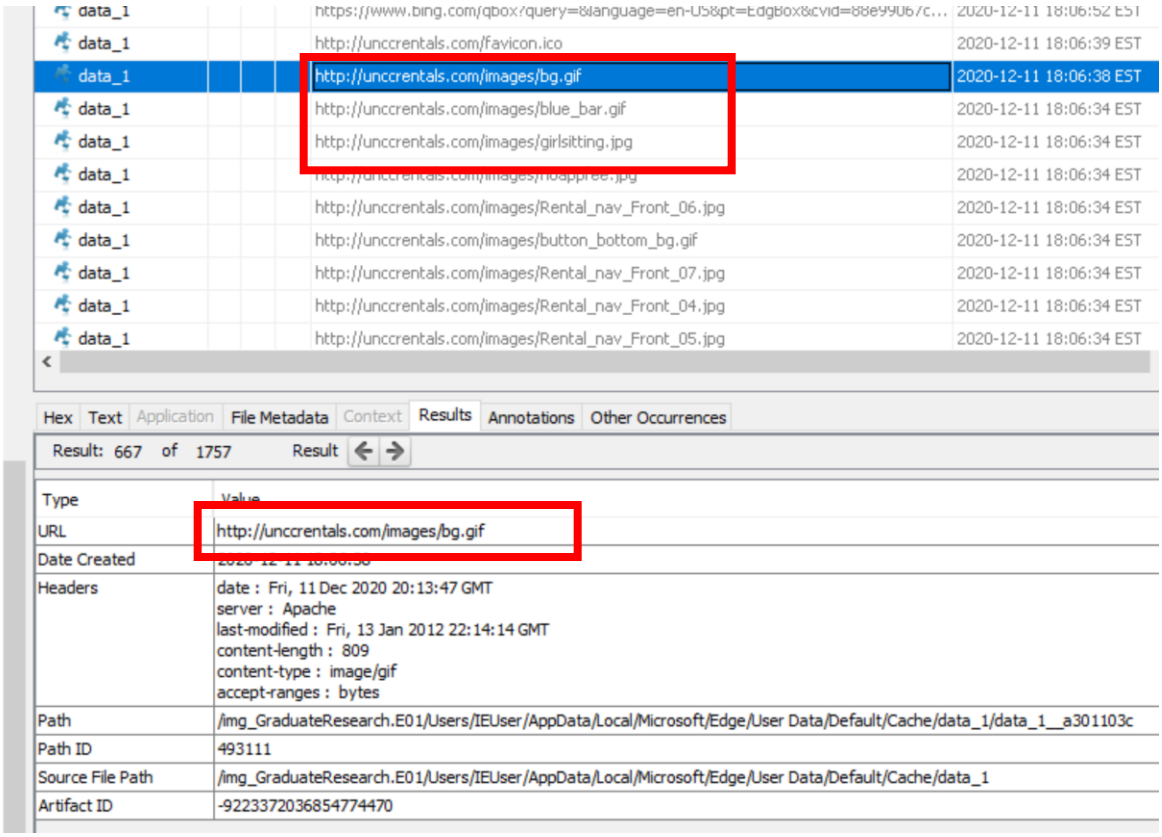
/img_GraduateResearch.E01/$Recycle.Bin/

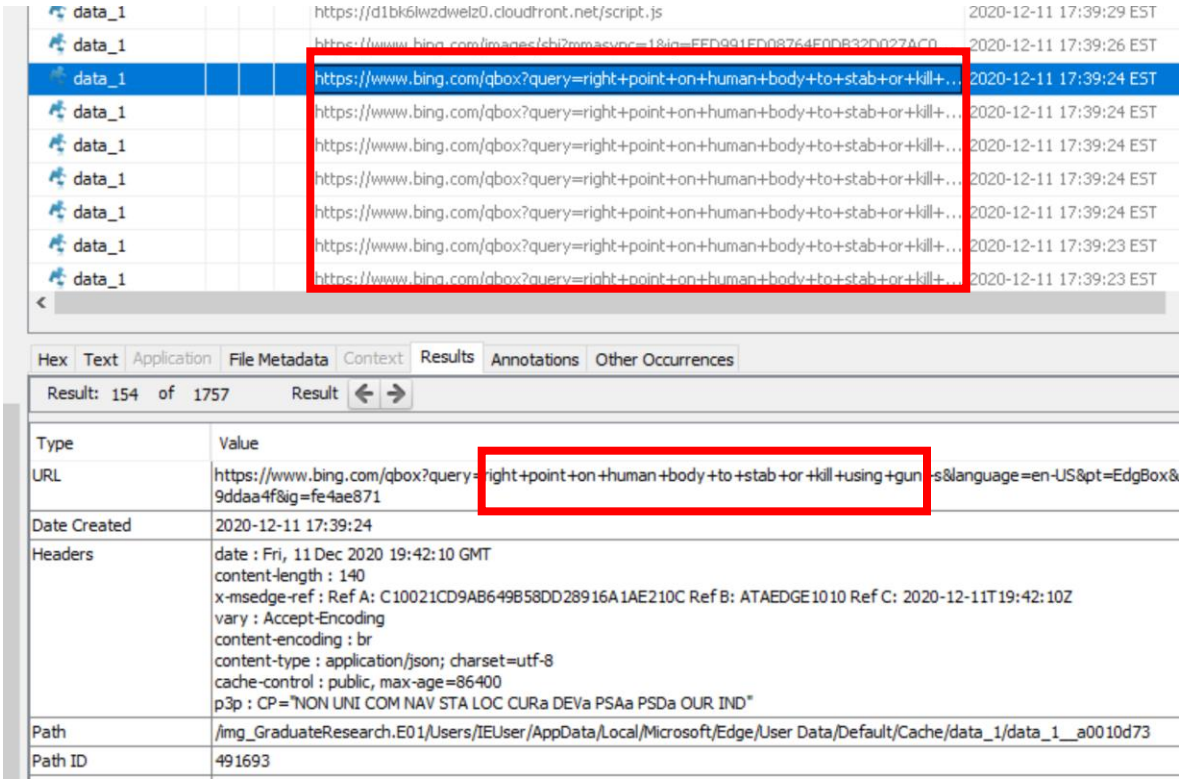


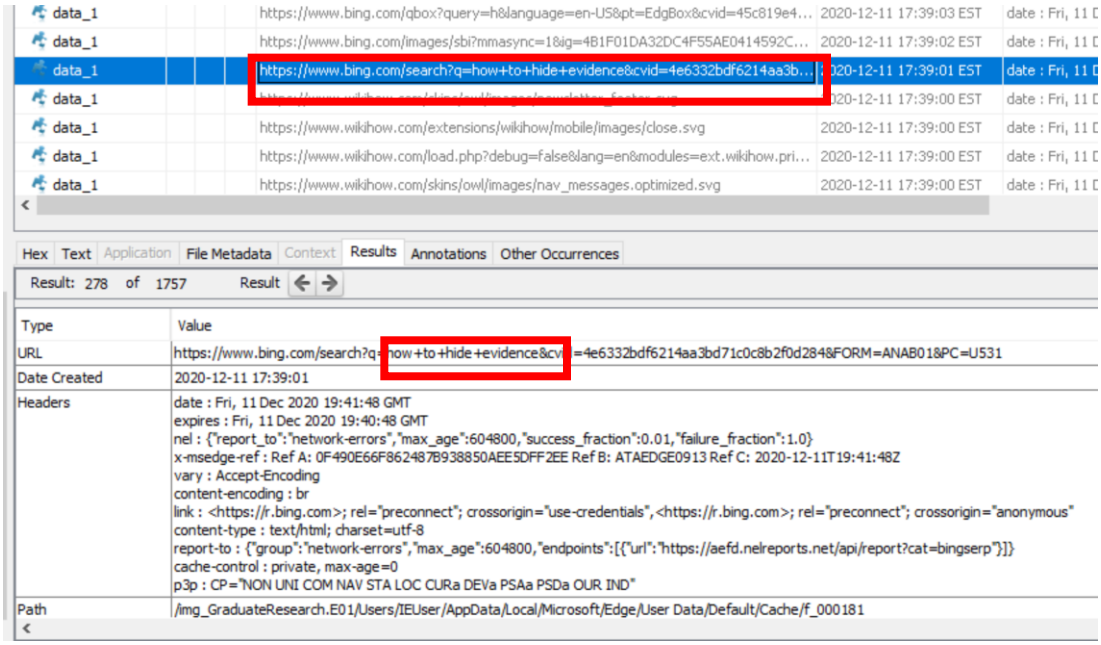
On analyzing the web searches using Autopsy, Hashbyte has done a lot of searches regarding the murder plan including **how to use the weapons, how to hack CCTV camera, how to brute force the Wi-Fi passwords and about the locations of UTN and Coffee Shop**.

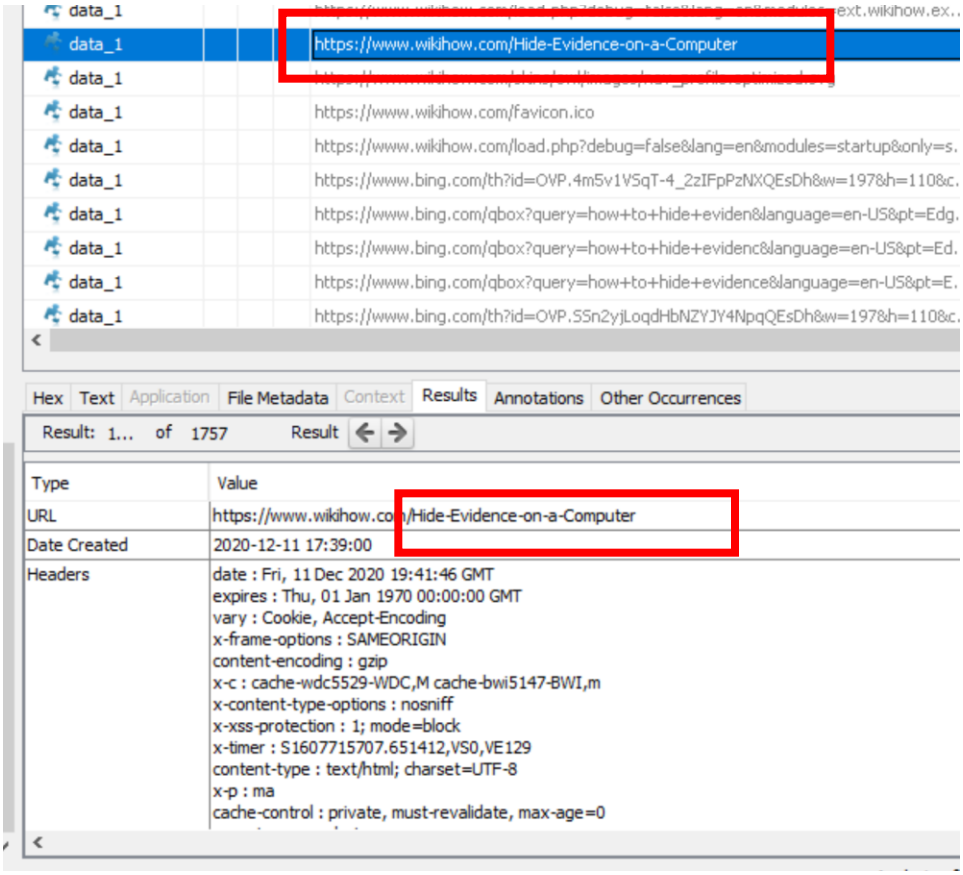

data_1 https://www.bing.com/qbox?query=http%3A%2F%2Futnapartments.com&language... 2020-12-11 18:07:42 EST
data_1 https://www.bing.com/qbox?query=http%3A%2F%2Futnapartments.c&language=e... 2020-12-11 18:07:42 EST
data_1 https://www.bing.com/qbox?query=http%3A%2F%2Futnapartments.co&language=... 2020-12-11 18:07:42 EST
data_1 https://www.bing.com/qbox?query=http%3A%2F%2Futnapartments&language=en-... 2020-12-11 18:07:41 EST
data_1 https://www.bing.com/qbox?query=http%3A%2F%2Futnapartments.&language=en... 2020-12-11 18:07:41 EST
data_1 https://www.bing.com/qbox?query=http%3A%2F%2Futnapartmen&language=en-U... 2020-12-11 18:07:40 EST
data_1 https://www.bing.com/qbox?query=http%3A%2F%2Futnapart&language=en-US&pt... 2020-12-11 18:07:40 EST
data_1 https://www.bing.com/qbox?query=http%3A%2F%2Futnapa&language=en-US&pt=... 2020-12-11 18:07:39 EST
data_1 2020-12-11 18:07:39 EST
data_1 https://www.bing.com/qbox?query=http%3A%2F%2Futnap&language=en-US&pt=E... 2020-12-11 18:07:39 EST
data_1 https://www.bing.com/qbox?query=http%3A%2F%2Futn&language=en-US&pt=Edg... 2020-12-11 18:07:36 EST
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.c&language=en-US&pt=EdgBox&cvid=37ca9f68177d4aae9bb1 4a61ad5bcee2bdd0f1f08&
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

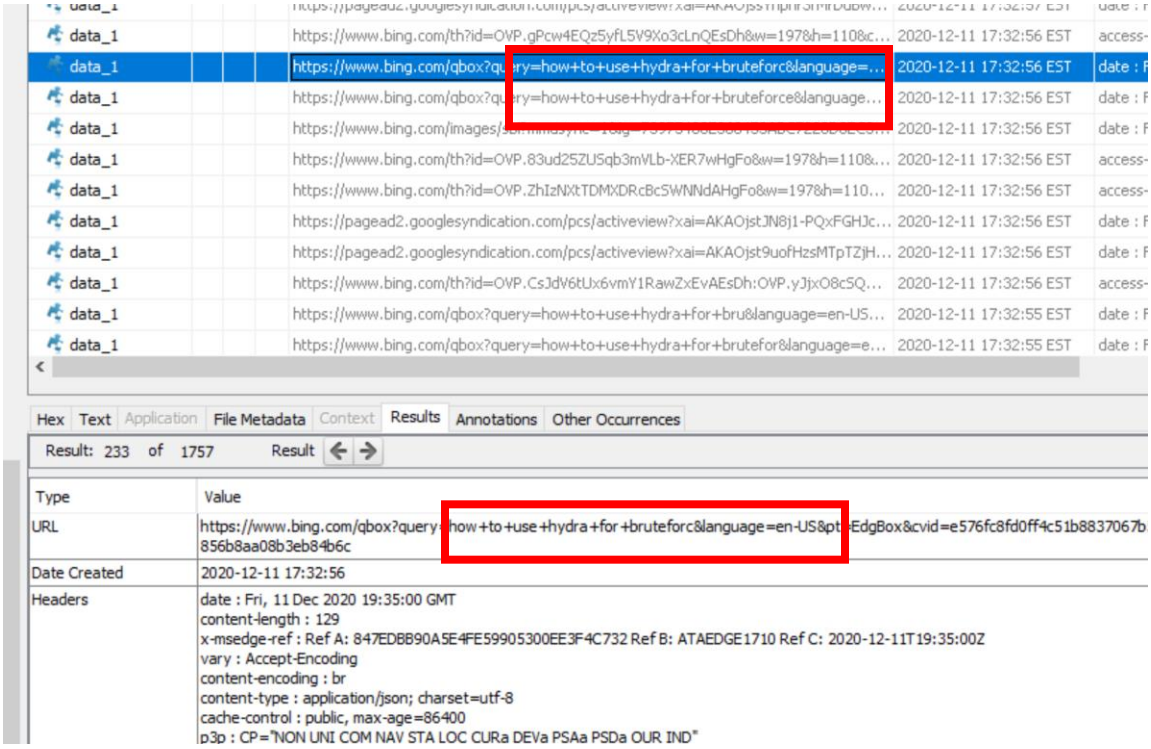

data_1 https://www.bing.com/qbox?query=http%3A%2F%2Fccdcoffeeshop.c&language=e... 2020-12-11 18:07:05 EST
data_1 2020-12-11 18:07:03 EST
data_1 https://www.bing.com/qbox?query=http%3A%2F%2Fccdcoffeesho&language=en-U... 2020-12-11 18:07:03 EST
data_1 https://www.bing.com/qbox?query=http%3A%2F%2Fccdcoffeeshop&language=en-... 2020-12-11 18:07:03 EST
data_1 https://www.bing.com/qbox?query=http%3A%2F%2Fccdcoffees&language=en-US&... 2020-12-11 18:07:02 EST
data_1 https://www.bing.com/qbox?query=http%3A%2F%2Fccdcoffee&language=en-US&p... 2020-12-11 18:07:01 EST
data_1 https://www.bing.com/qbox?query=http%3A%2F%2Fccdcoffe&language=en-US&pt... 2020-12-11 18:07:01 EST
data_1 2020-12-11 18:06:59 EST
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%2Fccdcoffeesho&language=en-US&pt=EdgBox&cvid=88e99067cc264de98 7b9f94296bc60bcd4&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

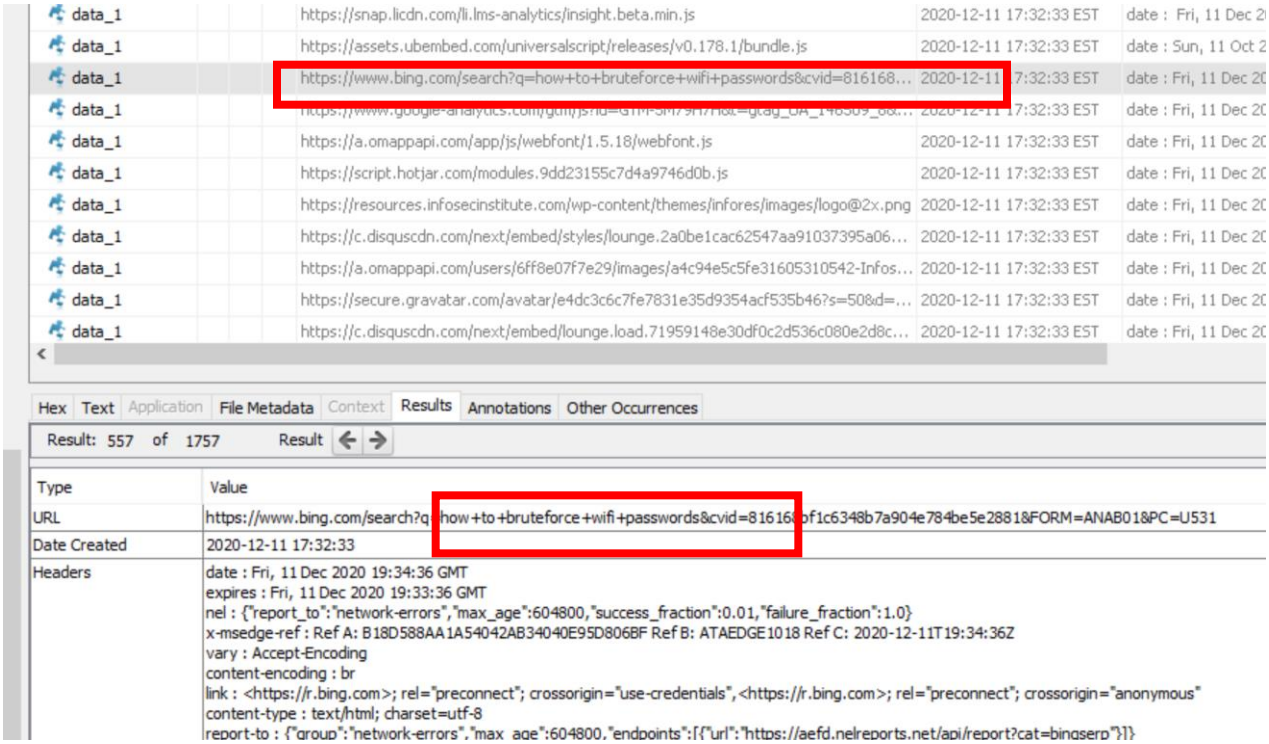

data_1 http://unccrentals.com/favicon.ico 2020-12-11 18:06:39 EST
data_1 http://unccrentals.com/images/bg.gif 2020-12-11 18:06:38 EST
data_1 http://unccrentals.com/images/blue_bar.gif 2020-12-11 18:06:34 EST
data_1 http://unccrentals.com/images/girlsitting.jpg 2020-12-11 18:06:34 EST
data_1 http://unccrentals.com/images/Rental_nav_Front_06.jpg 2020-12-11 18:06:34 EST
data_1 http://unccrentals.com/images/button_bottom_bg.gif 2020-12-11 18:06:34 EST
data_1 http://unccrentals.com/images/Rental_nav_Front_07.jpg 2020-12-11 18:06:34 EST
data_1 http://unccrentals.com/images/Rental_nav_Front_04.jpg 2020-12-11 18:06:34 EST
data_1 http://unccrentals.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://unccrentals.com/images/bg.gif
Date Created
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/IEUser/AppData/Local/Microsoft/Edge/User Data/Default/Cache/data_1/data_1__a301103c
Path ID 493111
Source File Path /img_GraduateResearch.E01/Users/IEUser/AppData/Local/Microsoft/Edge/User Data/Default/Cache/data_1
Artifact ID -9223372036854774470


data_1 https://d1bk6lwzdwelz0.cloudfront.net/script.js 2020-12-11 17:39:29 EST
data_1 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 17:39:24 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 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-s&language=en-US&pt=EdgBox&
9ddaa4f8&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 PSAa PSDa OUR IND"
Path /img_GraduateResearch.E01/Users/IEUser/AppData/Local/Microsoft/Edge/User Data/Default/Cache/data_1/data_1__a0010d73
Path ID 491693


data_1 https://www.bing.com/qbox?query=h&language=en-US&pt=EdgBox&cvid=45c819e4... 2020-12-11 17:39:03 EST date : Fri, 11 D
data_1 https://www.bing.com/images/sbi?mmasync=1&ig=4B1F01DA32DC4F55AE0414592C... 2020-12-11 17:39:02 EST date : Fri, 11 D
data_1 https://www.bing.com/search?q=how+to+hide+evidence&cvid=4e6332bdf6214aa3b... 2020-12-11 17:39:01 EST date : Fri, 11 D
data_1 2020-12-11 17:39:00 EST date : Fri, 11 D
data_1 https://www.wikihow.com/extensions/wikihow/mobile/images/close.svg 2020-12-11 17:39:00 EST date : Fri, 11 D
data_1 https://www.wikihow.com/load.php?debug=false&lang=en&modules=ext.wikihow.pri... 2020-12-11 17:39:00 EST date : Fri, 11 D
data_1 https://www.wikihow.com/skins/owl/images/nav_messages.optimized.svg 2020-12-11 17:39:00 EST date : Fri, 11 D
Hex Text Application File Metadata Context Results Annotations Other Occurrences
Result: 278 of 1757 Result
Type Value
URL https://www.bing.com/search?q=how+to+hide+evidence&cvid=4e6332bdf6214aa3bd71c0c8b2f0d2848&FORM=ANAB01&PC=U531
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 : <https://r.bing.com>; rel="preconnect"; crossorigin="use-credentials",<https://r.bing.com>; 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

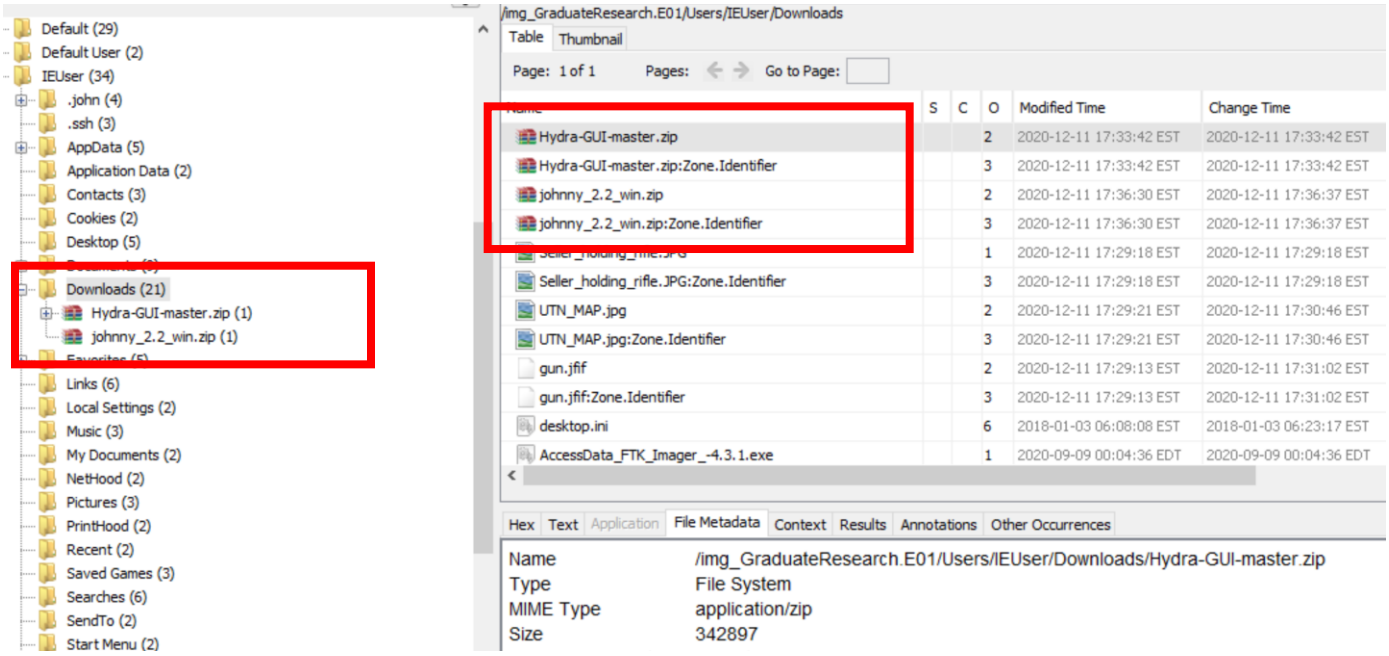

data_1 https://www.wikihow.com/Hide-Evidence-on-a-Computer
data_1 https://www.wikihow.com/favicon.ico
data_1 https://www.wikihow.com/load.php?debug=false&lang=en&modules=startup&only=s.
data_1 https://www.bing.com/th?id=OVP.4m5v1VSqT-4_2zIFpPzNXQEsDh&w=197&h=110&c.
data_1 https://www.bing.com/qbox?query=how+to+hide+eviden&language=en-US&pt=Edg.
data_1 https://www.bing.com/qbox?query=how+to+hide+evidenc&language=en-US&pt=Ed.
data_1 https://www.bing.com/qbox?query=how+to+hide+evidence&language=en-US&pt=E.
data_1 https://www.bing.com/th?id=OVP.5Sn2yjLoqdHbNZYJY4NpqQEsDh&w=197&h=110&c.
Hex Text Application File Metadata Context Results Annotations Other Occurrences
Result: 1... of 1757 Result
Type Value
URL https://www.wikihow.com/Hide-Evidence-on-a-Computer
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 https://www.bing.com/th?id=OVP.gPcw4EQz5yfL5V9Xo3cLnQEsDh&w=197&h=110&c... 2020-12-11 17:32:56 EST access-
data_1 https://www.bing.com/qbox?query=how+to+use+hydra+for+bruteforc&language=... 2020-12-11 17:32:56 EST date : F
data_1 https://www.bing.com/qbox?query=how+to+use+hydra+for+bruteforce&language... 2020-12-11 17:32:56 EST date : F
data_1 https://www.bing.com/images/ 2020-12-11 17:32:56 EST date : F
data_1 https://www.bing.com/th?id=OVP.83ud25ZUSqb3mVLb-XER7wHgFo&w=197&h=110&... 2020-12-11 17:32:56 EST access-
data_1 https://www.bing.com/th?id=OVP.ZhIzNXtTDMXDRcBcSWNNdAHgFo&w=197&h=110... 2020-12-11 17:32:56 EST access-
data_1 https://pagead2.googlesyndication.com/pcs/activeview?xai=AKAOjstJN8j1-PQxFGHJc... 2020-12-11 17:32:56 EST date : F
data_1 https://pagead2.googlesyndication.com/pcs/activeview?xai=AKAOjst9uofHzsMTpTZjH... 2020-12-11 17:32:56 EST date : F
data_1 https://www.bing.com/th?id=OVP.CsJdV6tUx6vmY1RawZxEvAEsDh:OVP.yJjxO8c5Q... 2020-12-11 17:32:56 EST access-
data_1 https://www.bing.com/qbox?query=how+to+use+hydra+for+bru&language=en-US... 2020-12-11 17:32:55 EST date : F
data_1 https://www.bing.com/qbox?query=how+to+use+hydra+for+bruteforc&language=e... 2020-12-11 17:32:55 EST date : F
Hex Text Application File Metadata Context Results Annotations Other Occurrences
Result: 233 of 1757 Result
Type Value
URL https://www.bing.com/qbox?query=how+to+use+hydra+for+bruteforc&language=en-US&pt=EdgBox&cvid=e576fc8fd0ff4c51b8837067b856b8aa08b3eb84b6c
Date Created 2020-12-11 17:32:56
Headers date : Fri, 11 Dec 2020 19:35:00 GMT
content-length : 129
x-msedge-ref : Ref A: 847EDBB90A5E4FE59905300EE3F4C732 Ref B: ATAEDGE1710 Ref C: 2020-12-11T19:35:00Z
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"

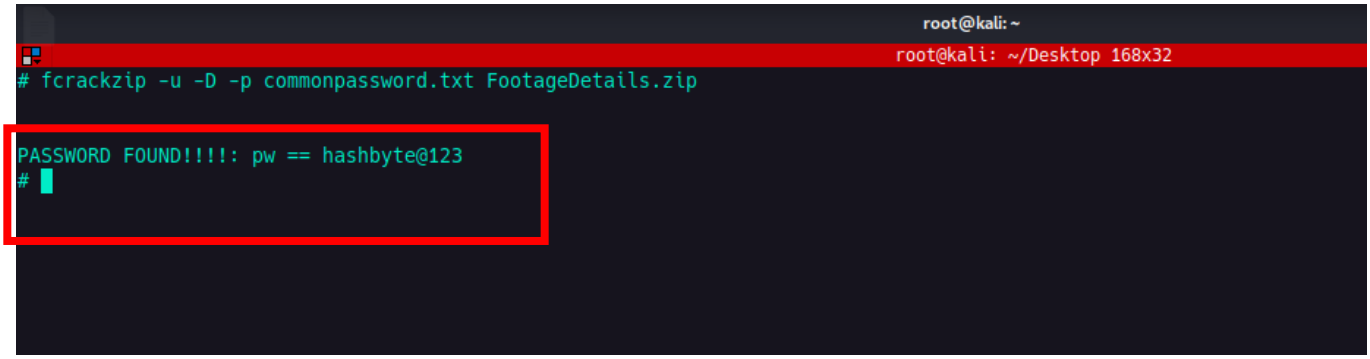

data_1 https://snap.licdn.com/li.lms-analytics/insight.beta.min.js 2020-12-11 17:32:33 EST date : Fri, 11 Dec 2
data_1 https://assets.ubembed.com/universalscript/releases/v0.178.1/bundle.js 2020-12-11 17:32:33 EST date : Sun, 11 Oct 2
data_1 https://www.bing.com/search?q=how+to+bruteforce+wifi+passwords&cvid=816168... 2020-12-11 17:32:33 EST date : Fri, 11 Dec 20
data_1 https://www.google-analytics.com/gtm/js?id=GTM-SM79H7N&l=gtag_UA_148389_8&... 2020-12-11 17:32:33 EST date : Fri, 11 Dec 20
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 20
data_1 https://script.hotjar.com/modules.9dd23155c7d4a9746d0b.js 2020-12-11 17:32:33 EST date : Fri, 11 Dec 20
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 20
data_1 https://c.disquscdn.com/next/embed/styles/lounge.2a0be1cac62547aa91037395a06... 2020-12-11 17:32:33 EST date : Fri, 11 Dec 20
data_1 https://a.omappapi.com/users/6ff8e07f7e29/images/a4c94e5c5fe31605310542-Infos... 2020-12-11 17:32:33 EST date : Fri, 11 Dec 20
data_1 https://secure.gravatar.com/avatar/e4dc3c6c7fe7831e35d9354acf535b46?s=50&d=... 2020-12-11 17:32:33 EST date : Fri, 11 Dec 20
data_1 https://c.disquscdn.com/next/embed/lounge.load.71959148e30df0c2d536c080e2d8c... 2020-12-11 17:32:33 EST date : Fri, 11 Dec 20
Hex Text Application File Metadata Context Results Annotations Other Occurrences
Result: 557 of 1757 Result
Type Value
URL https://www.bing.com/search?q=how+to+bruteforce+wifi+passwords&cvid=816168bf1c6348b7a904e784be5e2881&FORM=ANAB01&PC=U531
Date Created 2020-12-11 17:32:33
Headers date : Fri, 11 Dec 2020 19:34:36 GMT
expires : Fri, 11 Dec 2020 19:33:36 GMT
nel : {"report_to":"network-errors","max_age":604800,"success_fraction":0.01,"failure_fraction":1.0}
x-msedge-ref : Ref A: B18D588AA1A54042AB34040E95D806BF Ref B: ATAEDGE1018 Ref C: 2020-12-11T19:34:36Z
vary : Accept-Encoding
content-encoding : br
link : <https://r.bing.com>; rel="preconnect"; crossorigin="use-credentials",<https://r.bing.com>; 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"}]}

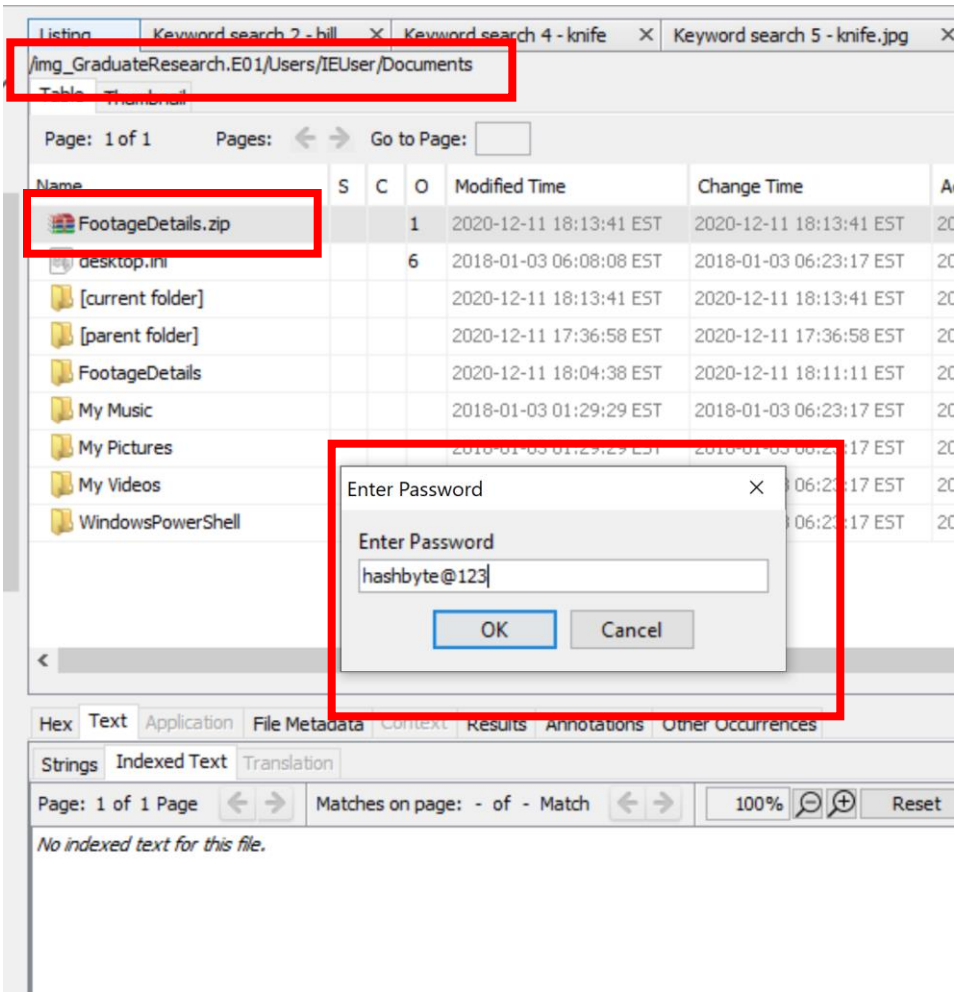
Password cracking tools like **Hydra and Johnny (John the Ripper)** were also downloaded and installed and were found in the "Downloads" Folder in the location

/img_GraduateResearch.E01/Users/IEUser/Downloads.

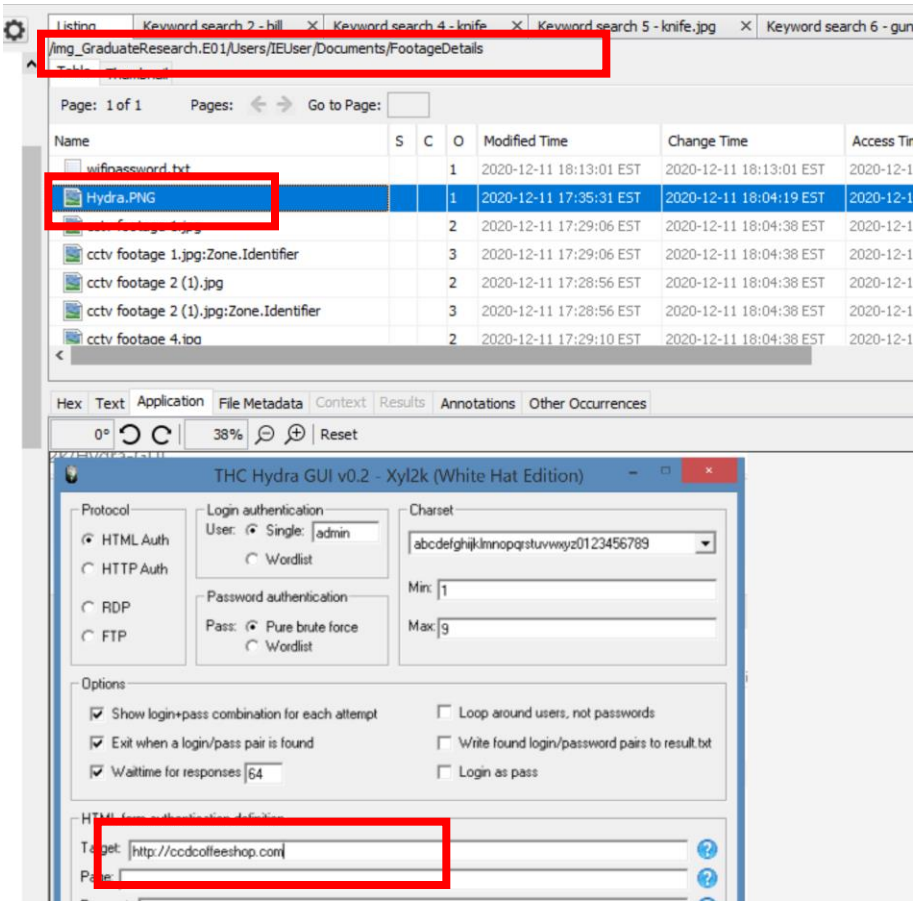


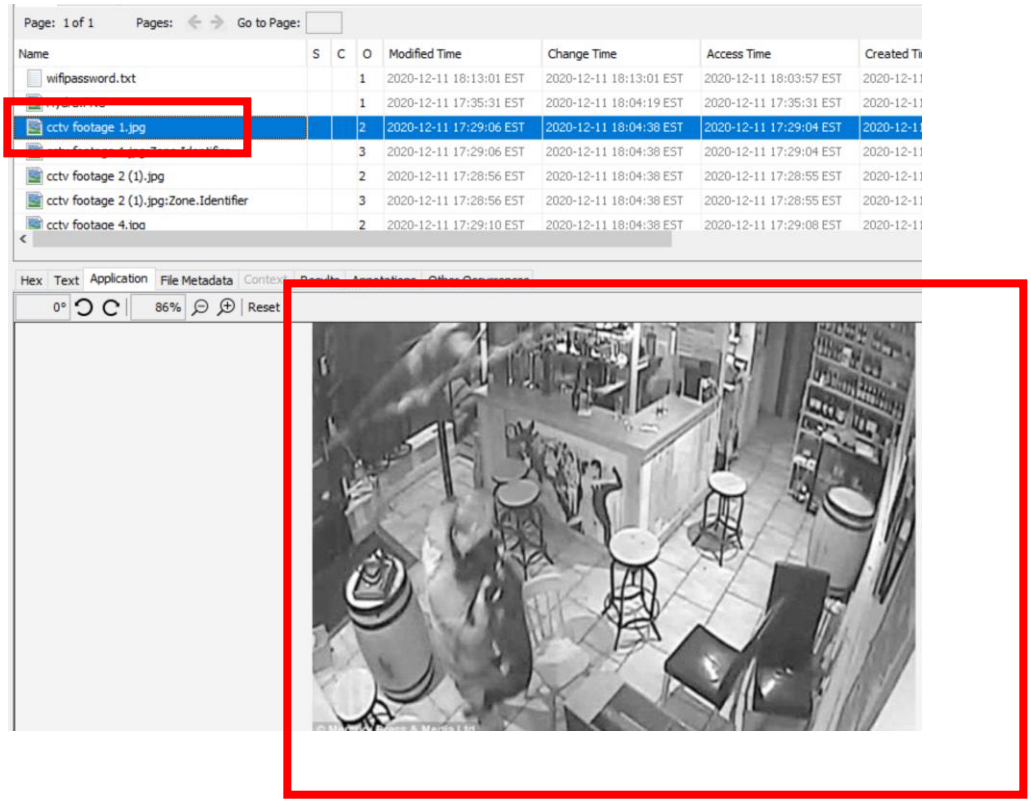
In the **"Documents"** folders, there was a password zipped file named **"FootageDetails.zip".** I cracked the password of the zip file using **fcrackzip v1.0** tool in my Kali Linux and found the password to be **hashbyte@123**



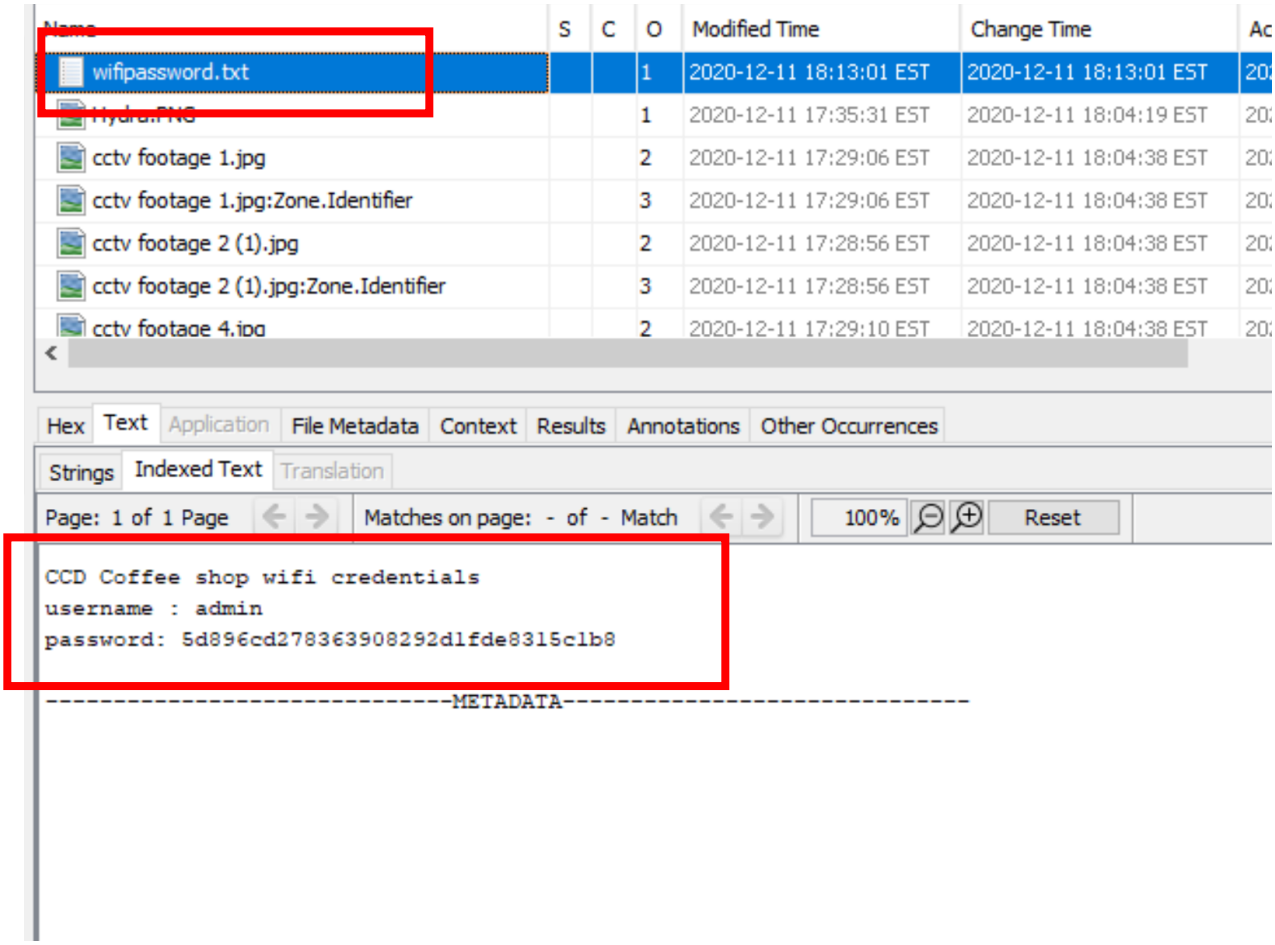


In the FootageDetails folder, there were pictures of **CCTV footages and Hydra** where the target was set to be http://ccdcoffeeshop.com to brute force the Wi-Fi password of the coffee shop using Hydra tool.


Keyword search 2 - hill
Keyword search 4 - knife
Keyword search 5 - knife.jpg
Keyword search 6 - gun
/img_GraduateResearch.E01/Users/IEUser/Documents/FootageDetails
Page: 1 of 1
Pages:
Go to Page:
Name
S
C
O
Modified Time
Change Time
Access Tir
wifipassword.txt
1
2020-12-11 18:13:01 EST
2020-12-11 18:13:01 EST
Hydra.PNG
1
2020-12-11 17:35:31 EST
2020-12-11 18:04:19 EST
2
2020-12-11 17:29:06 EST
2020-12-11 18:04:38 EST
cctv footage 1.jpg:Zone.Identifier
3
2020-12-11 17:29:06 EST
2020-12-11 18:04:38 EST
cctv footage 2 (1).jpg
2
2020-12-11 17:28:56 EST
2020-12-11 18:04:38 EST
cctv footage 2 (1).jpg:Zone.Identifier
3
2020-12-11 17:28:56 EST
2020-12-11 18:04:38 EST
cctv footage 4.jpg
2
2020-12-11 17:29:10 EST
2020-12-11 18:04:38 EST
Hex
Text
Application
File Metadata
Context
Results
Annotations
Other Occurrences
0°
38%
Reset
THC Hydra GUI v0.2 - Xyl2k (White Hat Edition)
Protocol
HTML Auth
HTTP Auth
RDP
FTP
Login authentication
User:
Single:
admin
Wordlist
Password authentication
Pass:
Pure brute force
Wordlist
Charset
abcdefghijklmnopqrstuvwxyz0123456789
Min:
1
Max:
9
Options
Show login+pass combination for each attempt
Exit when a login/pass pair is found
Waittime for responses
64
Loop around users, not passwords
Write found login/password pairs to result.txt
Login as pass
Target:
http://ccdcoffeeshop.com

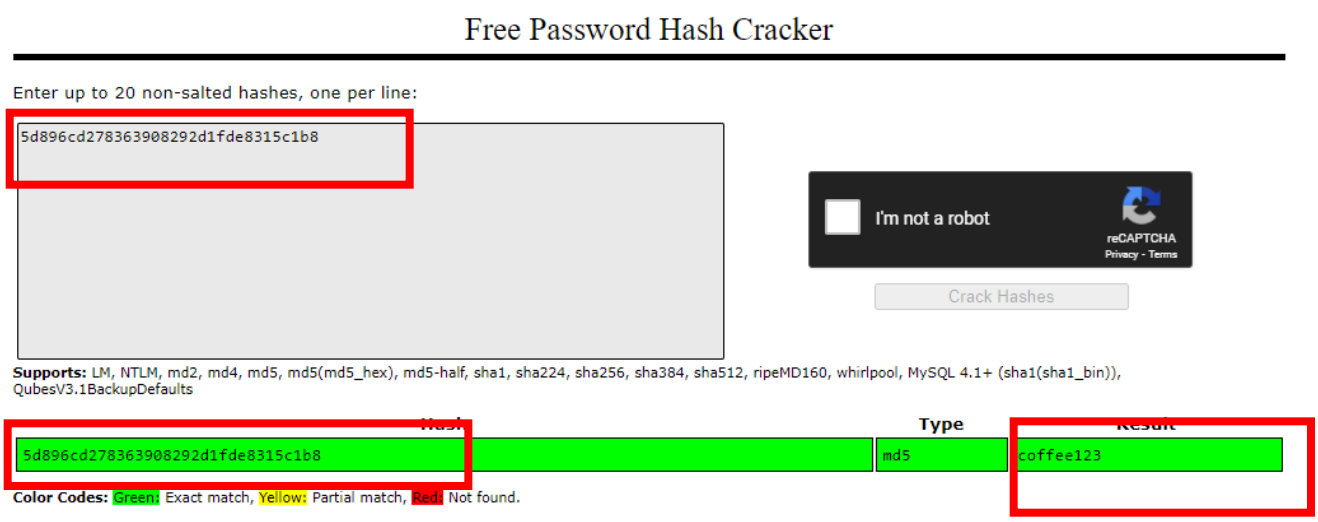

Page: 1 of 1
Pages:
Go to Page:
Name
S
C
O
Modified Time
Change Time
Access Time
Created Ti
wifipassword.txt
1
2020-12-11 18:13:01 EST
2020-12-11 18:13:01 EST
2020-12-11 18:03:57 EST
1
2020-12-11 17:35:31 EST
2020-12-11 18:04:19 EST
2020-12-11 17:35:31 EST
cctv footage 1.jpg
2
2020-12-11 17:29:06 EST
2020-12-11 18:04:38 EST
2020-12-11 17:29:04 EST
3
2020-12-11 17:29:06 EST
2020-12-11 18:04:38 EST
2020-12-11 17:29:04 EST
cctv footage 2 (1).jpg
2
2020-12-11 17:28:56 EST
2020-12-11 18:04:38 EST
2020-12-11 17:28:55 EST
cctv footage 2 (1).jpg:Zone.Identifier
3
2020-12-11 17:28:56 EST
2020-12-11 18:04:38 EST
2020-12-11 17:28:55 EST
cctv footage 4.jpg
2
2020-12-11 17:29:10 EST
2020-12-11 18:04:38 EST
2020-12-11 17:29:08 EST
Hex
Text
Application
File Metadata
0°
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**.

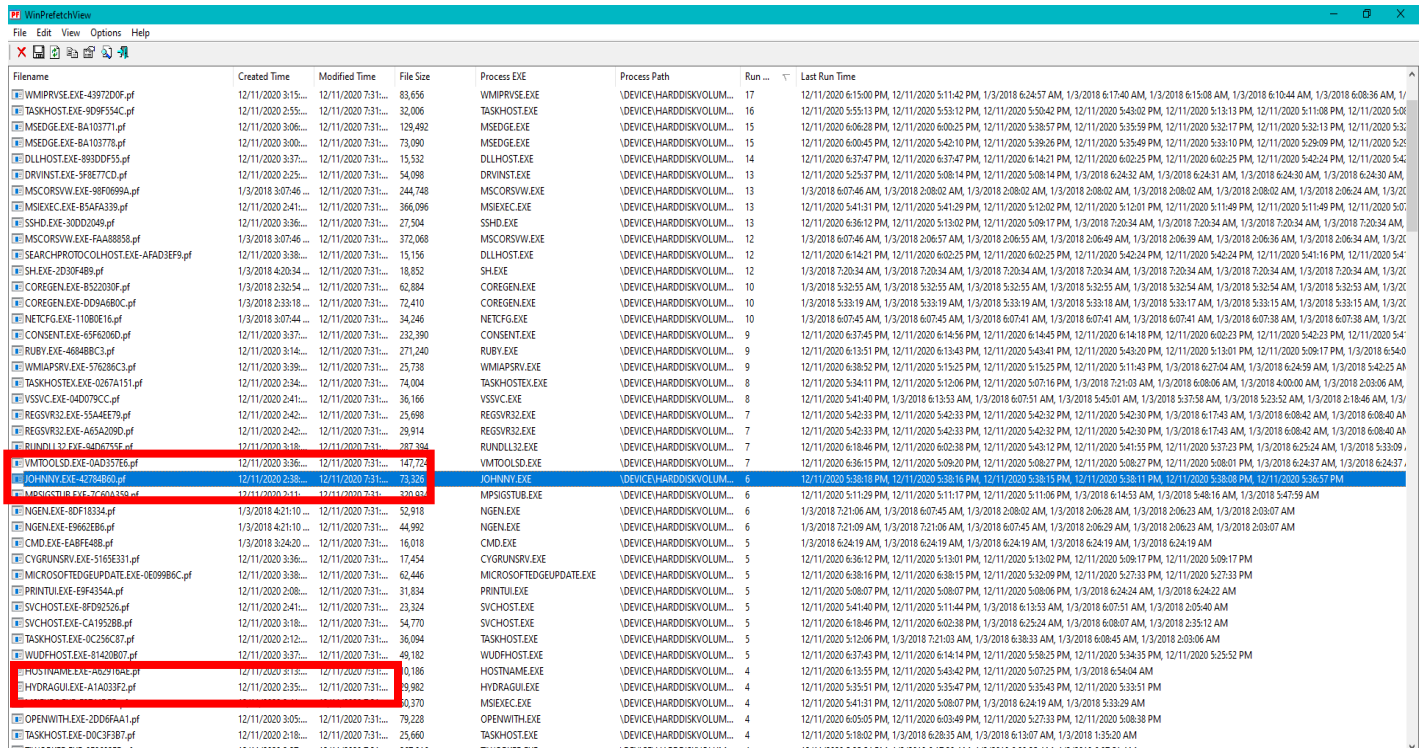


I was able to **crack the original value of the hash using an online tool – Crack Station.**

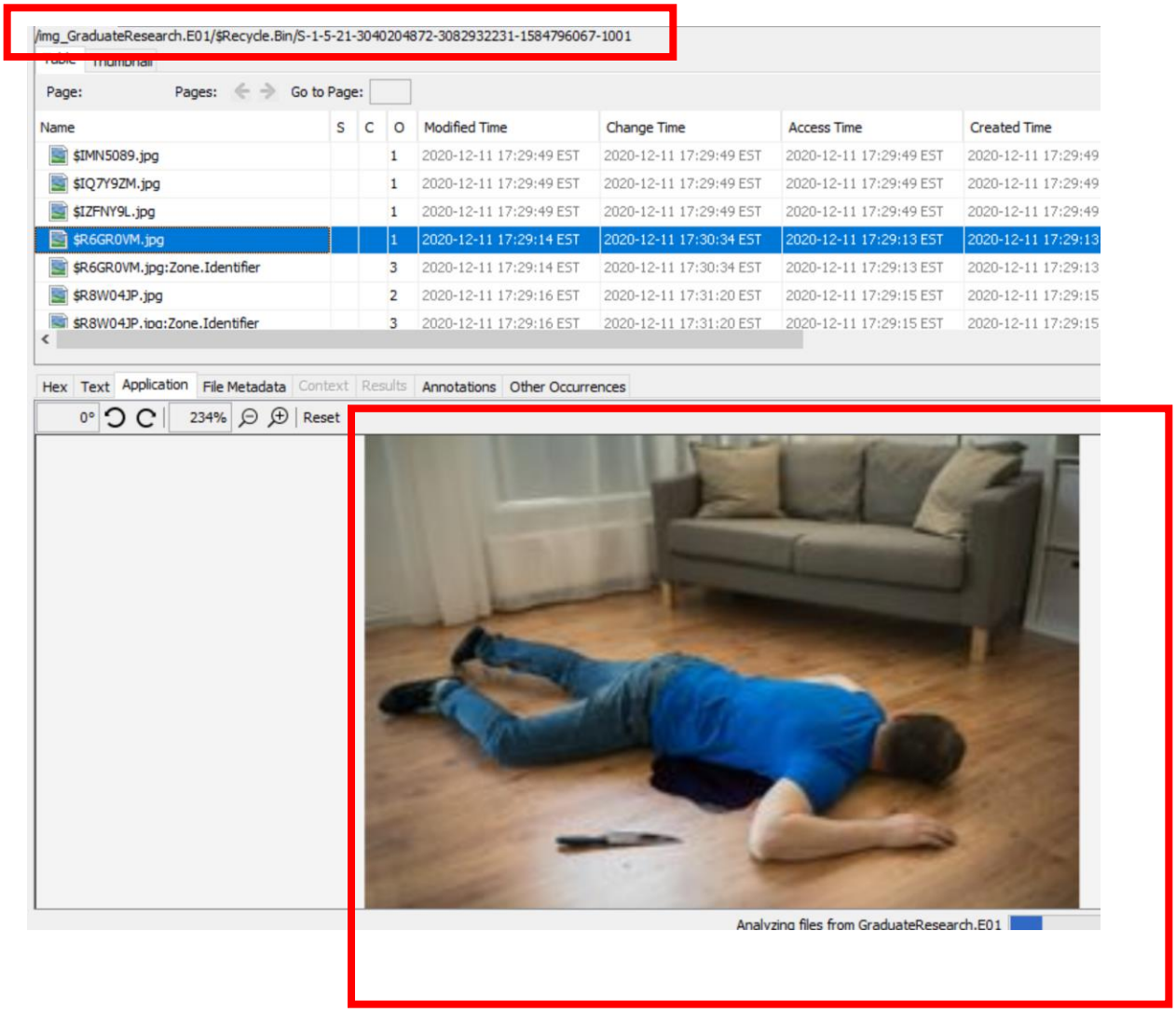
And found the password to be **coffee123**



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



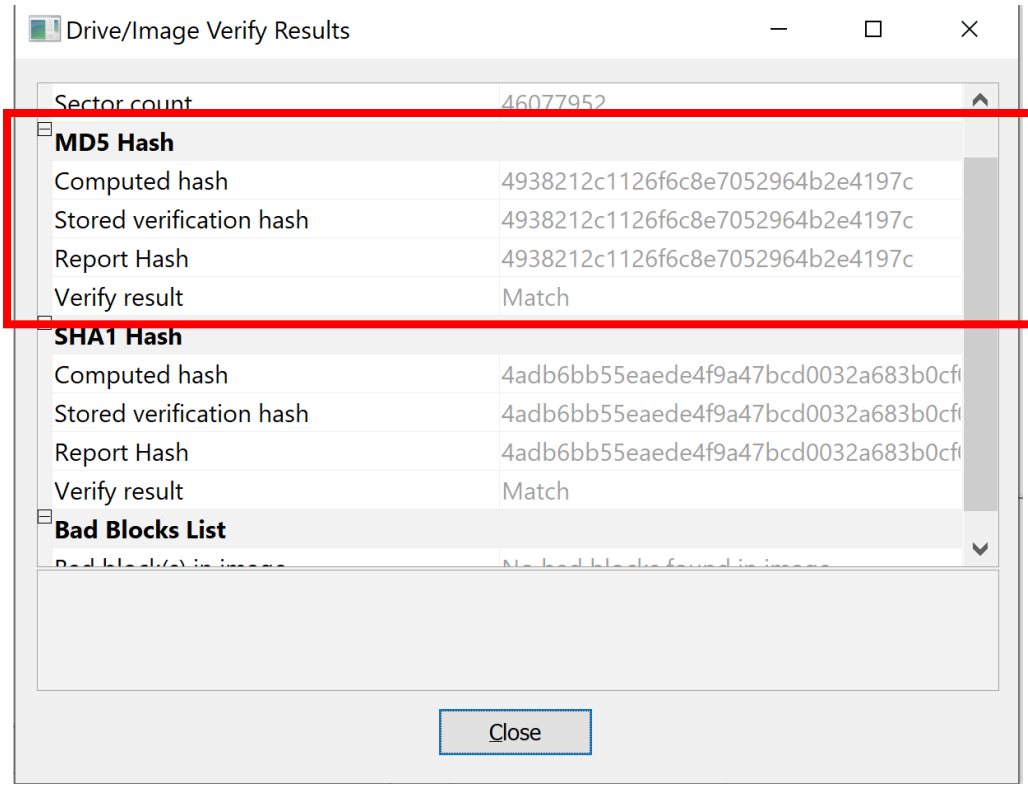
Finally, a **murder image** was also found in the Recycle Bin Folder.



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



Signed:

Vinitha Mathiyazhagan

DFE Vinitha Mathiyazhagan

Digital Forensics Examiner

UNCC Forensics Lab