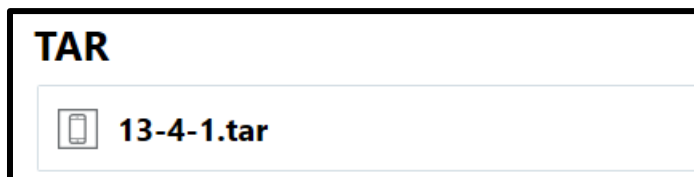
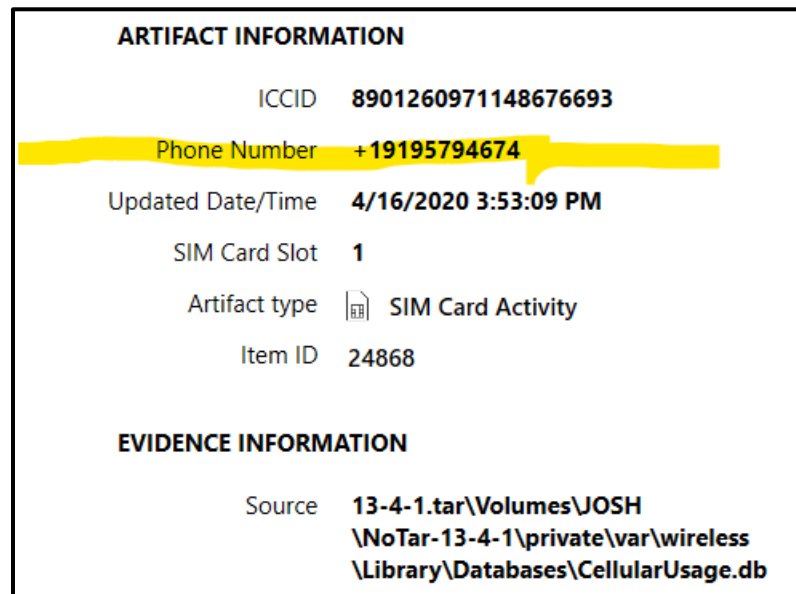


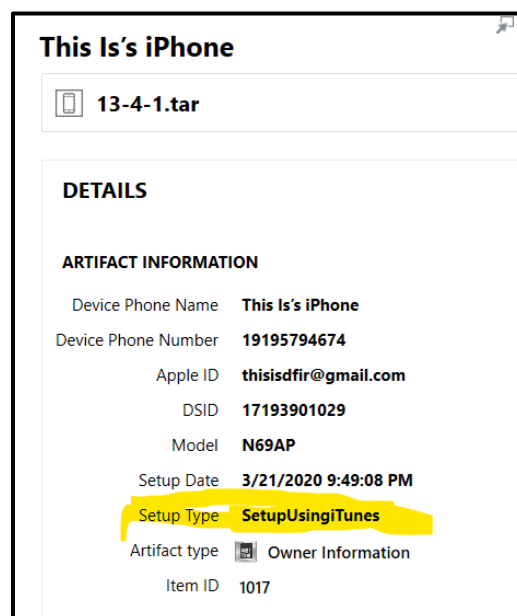
1. What is the serial number of the device?



2. What is the phone number of the device?




3. Was the phone set up using iTunes or iCloud?



4. How many different Apple Accounts are used on the phone?


Only 1 : this one is associated with an apple ID. Others under apple accounts are all services using the account associated with this apple ID.

thisisdffir@gmail.com

 **13-4-1.tar**

DETAILS

ARTIFACT INFORMATION

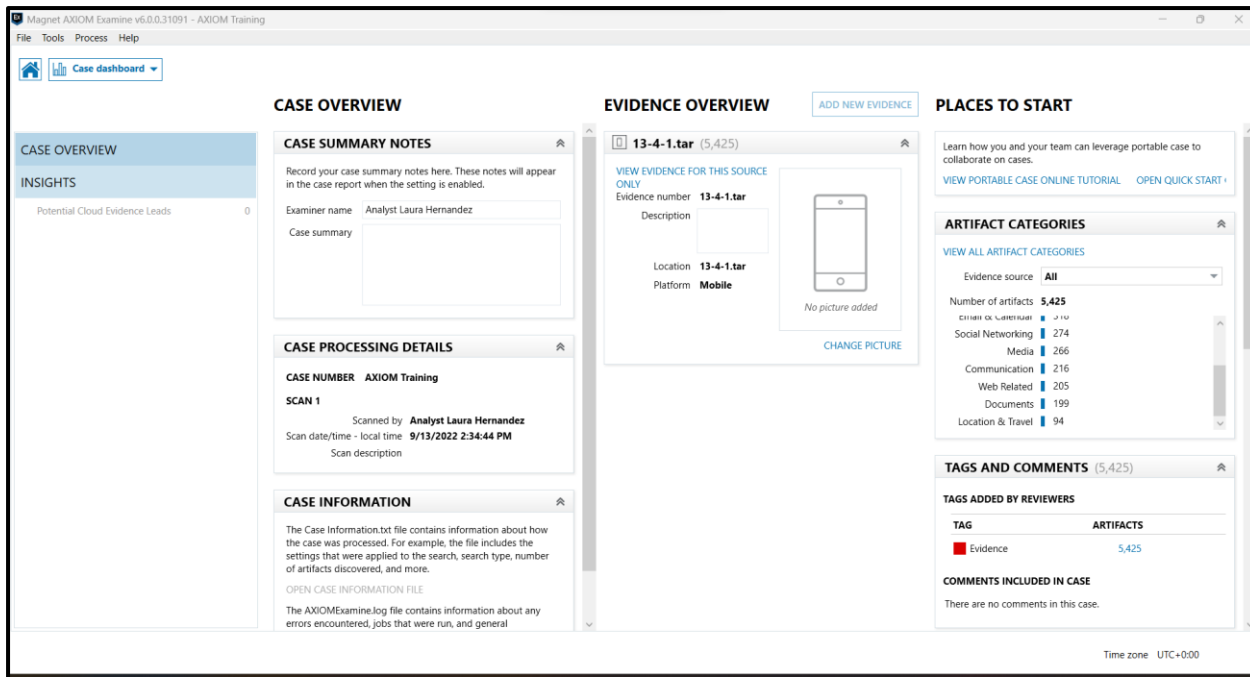
User Name	thisisdffir@gmail.com
Account ID	5B9A4BE7-A9AC-4798-A8EE-67EB19537748
Account Added Date/Time	3/21/2020 9:47:58 PM
Parent Account ID	03CF4555-027D-4CBB-87FD-462FC610F64D
Account Type	Apple ID
Account Credential Type	appleid-authentication
Owning Bundle ID	com.apple.AuthKit
Artifact type	 Apple Accounts
Item ID	5879

EVIDENCE INFORMATION

Source	13-4-1.tar\Volumes\JOSH \NoTar-13-4-1\private\var \mobile\Library\Accounts \Accounts3.sqlite
Recovery method	Parsing
Deleted source	

5. What four items are on the bottom of the home screen?

This is what my home screen looks like:



A panel to switch between case overview and insights

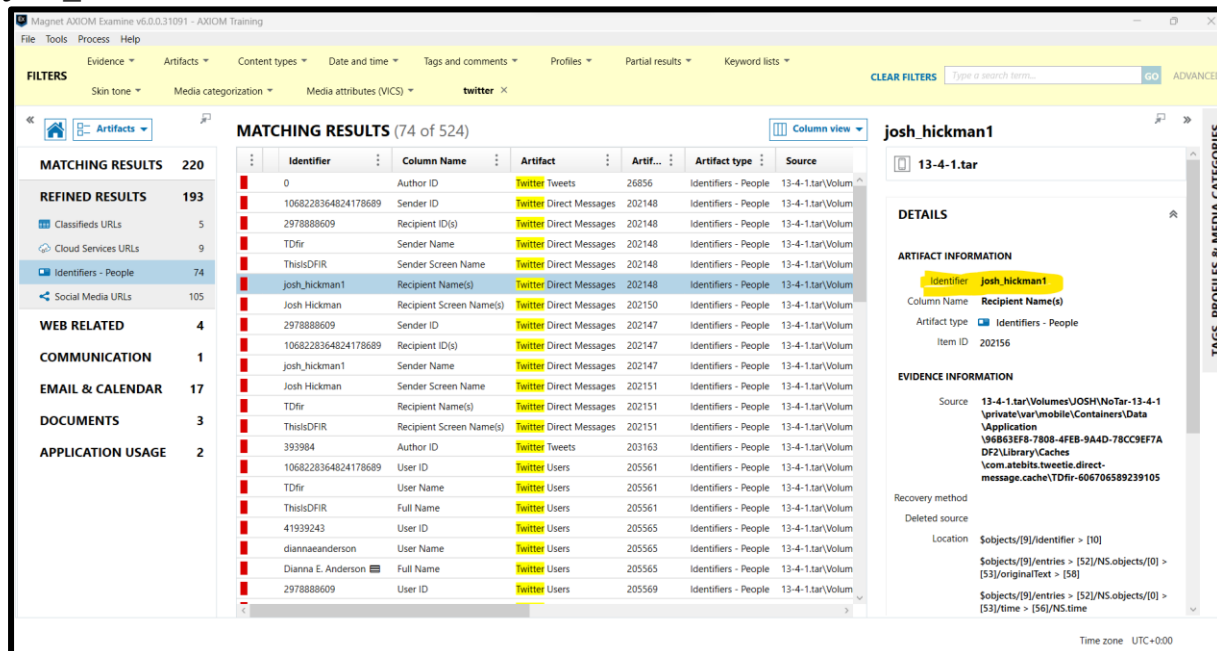
Case overview: information about the investigator and other case notes

Evidence overview: info about evidence(s) used in in the investigation process with their evidence numbers

Places to start pane: as the name says, summary of results and tags, etc.

6. What is Josh Hickman's Twitter Username?

josh_hickman1



7. On 4/16/2020, what alarms does the user have programmed (even if they are turned off)?

1 at 9:30 am (turned off)

Magnet AXIOM Examine v6.0.0.31091 - AXIOM Training

FileToolsProcessHelp

EvidenceArtifactsContent typesApr 15, 2020 - Apr 17,...Tags and commentsProfilesPartial resultsKeyword lists

FILTERS

Skin toneMedia categorizationMedia attributes (VICS)timer

CLEAR FILTERSType a search term...GOADVANCED

«HomeArtifacts»

MATCHING RESULTS2

MEDIA1

APPLICATION USAGE1

MATCHING RESULTS (2 of 5,425)

Column view

Item ID	Item	Artifact type	Artifact cat...	Date and time
47092	com.apple.mobiletimer	KnowledgeC Application U...	Application Usage	4/16/2020 12:11:24 PM
192372	com.apple.mobiletimer	iOS Snapshots	Media	4/16/2020 12:11:26 PM

com.apple.mobiletimer

13-4-1.tar

PREVIEW

Edit+

Alarm

9:30AM

Test Alarm

Time zoneUTC+0:00

8. The user has a photo storage app installed that can be locked with a passcode. When was the app installed? Bonus: what is the password or PIN that can be used to unlock albums on the app?

com.enchantedcloud.photovault

13-4-1.tar

DETAILS

ARTIFACT INFORMATION

Package Name

com.enchantedcloud.photovault

Installed Date/Time

4/14/2020 1:14:20 AM

Internal Version

10.5

Display Name

PhotoVault

Display Version

10.5

AppSource

/private/var/containers/Bundle/ Application/C746C5D2-1095-4428- B43E-34312EF056D9/ PhotoVault.app

Application Data

/private/var/mobile/Containers/ Data/Application/C4CC2E81- A70D-41C6-A3C9-03F7A02530A0

Type

User

Artifact type

Installed Applications

Item ID

13978

EVIDENCE INFORMATION

Source

13-4-1.tar\Volumes\JOSH \NoTar-13-4-1\private\var\mobile \Library\FrontBoard

Apple watch

The screenshot displays the details of an artifact named '13-4-1.tar'. At the top, the MAC address 'F8:6F:C1:4E:FF:6A' is shown. Below this, the artifact is identified as an 'Apple Watch' with a 'Bluetooth Devices' type and an 'Item ID' of '173250'. The 'EVIDENCE INFORMATION' section provides the source path: '13-4-1.tar\Volumes\JOSH\NoTar-13-4-1\private\var\containers\Shared\SystemGroup\9140AD4D-45D5-49D5-8AA8-1CD264CF295D\Library\Preferences\com.apple.MobileBluetooth.devices.plist'. It also lists the 'Recovery method' as 'Parsing', the 'Deleted source' as 'Location', and the 'Evidence number' as '13-4-1.tar'.

F8:6F:C1:4E:FF:6A	
13-4-1.tar	
DETAILS	
ARTIFACT INFORMATION	
MAC Address	F8:6F:C1:4E:FF:6A
Name	Apple Watch
Artifact type	Bluetooth Devices
Item ID	173250
EVIDENCE INFORMATION	
Source	13-4-1.tar\Volumes\JOSH\NoTar-13-4-1\private\var\containers\Shared\SystemGroup\9140AD4D-45D5-49D5-8AA8-1CD264CF295D\Library\Preferences\com.apple.MobileBluetooth.devices.plist
Recovery method	Parsing
Deleted source	Location
Location	n/a
Evidence number	13-4-1.tar

10. How many people does the user follow on Instagram that do not follow him back?

Total 4

Magnet AXIOM Examine v6.0.0.31091 - AXIOM Training

FileToolsProcessHelp

EvidenceArtifactsContent typesDate and timeTags and commentsProfilesPartial resultsKeyword listsSkin tone

Type a search term...GOADVANCED

FILTERS

Media categorizationMedia attributes (VICS)

Artifacts

EVIDENCE (5)

Column view

	User Name	Name	User...	Profile Picture URL	Loca...
	thisisdfr			https://scontent-iad3-1.cdninstagram.com/v/t51.28...	
	natgeotravel	National Geographic Travel	23947096	https://scontent-iad3-1.cdninstagram.com/v/t51.28...	9368974384
	josh_hickman	josh_hickman	22824420	https://scontent-iad3-1.cdninstagram.com/v/t51.28...	9368974384
	historyloversclub	History Lovers Club	3542039913	https://scontent-iad3-1.cdninstagram.com/v/t51.28...	9368974384
	thedad	The Dad	1153936614	https://scontent-iad3-1.cdninstagram.com/v/t51.28...	9368974384

natgeotravel

13-4-1.tar

DETAILS

ARTIFACT INFORMATION

User Name: natgeotravel

Name: National Geographic Travel

User ID: 23947096

Profile Picture URL: https://scontent-iad3-1.cdninstagram.com/v/t51.2885-19/s150x150/75328498_1674845792651317_2836767341423886336_n.jpg?_nc_ht=scontent-iad3-1.cdninstagram.com&_nc_ohc=96J879ORI3cAX9Coyff&oh=4943967b10c84e8ed2e391af4f92d5b9&oe=5EC1766D

Local User: 9368974384

Following: Yes

Is Followed By: No

Post Notifications: No

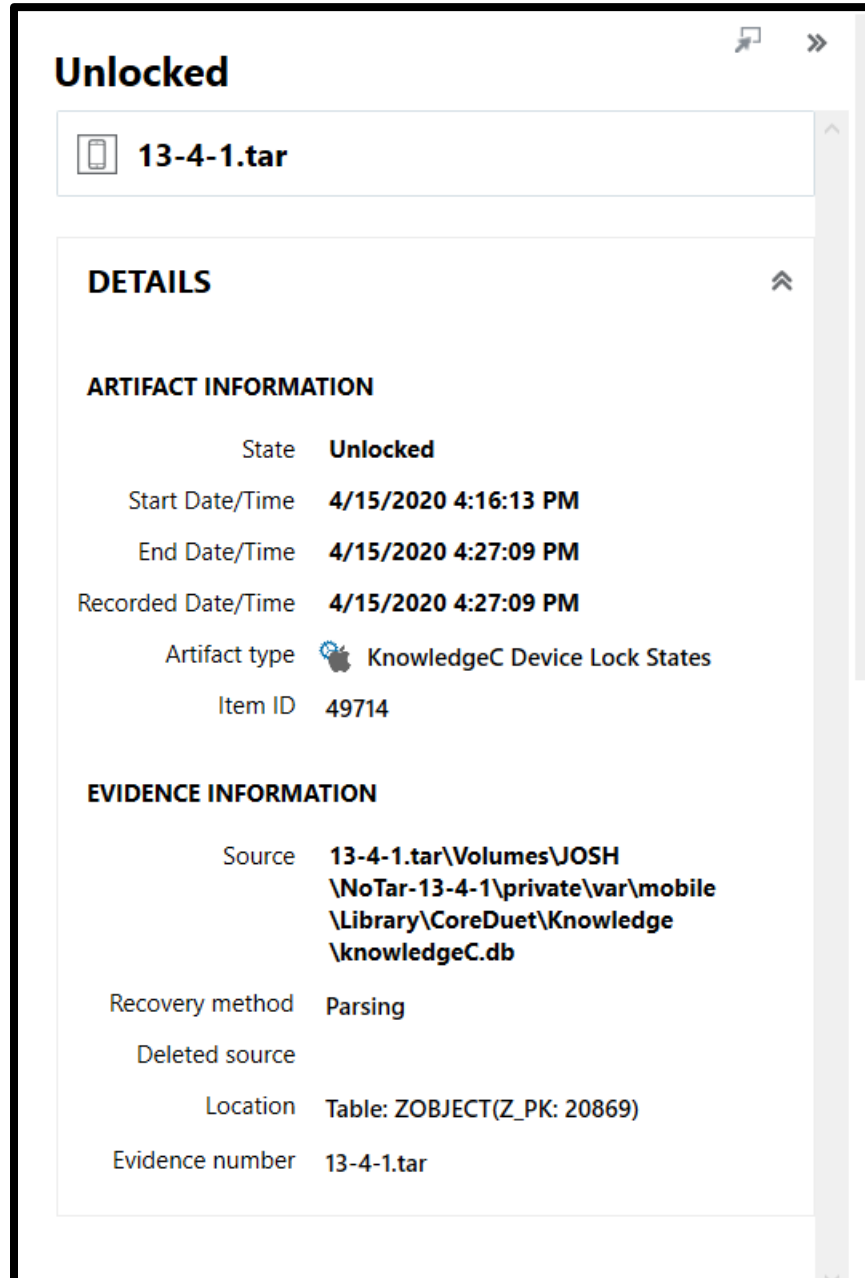
Artifact type: Instagram Profiles

Item ID: 197180

EVIDENCE INFORMATION

Time zone: UTC+0:00

Unlocked :



Plugged in :

Plugged in

13-4-1.tar

DETAILS

ARTIFACT INFORMATION

State

Plugged in

Start Date/Time

4/15/2020 4:16:15 PM


End Date/Time

4/15/2020 4:22:53 PM

Recorded Date/Time

4/15/2020 4:22:54 PM

Artifact type

 KnowledgeC Device Plugged-in States

Item ID

51789

EVIDENCE INFORMATION

Source

13-4-1.tar\Volumes\JOSH
\NoTar-13-4-1\private\var\mobile
\Library\CoreDuet\Knowledge
\knowledgeC.db

Recovery method

Parsing

Deleted source

Location


Table: ZOBJECT(Z_PK: 20852)

Evidence number

13-4-1.tar

Screen on:

Screen on

 13-4-1.tar

DETAILS

ARTIFACT INFORMATION

State

Screen on

Start Date/Time

4/15/2020 4:16:00 PM


End Date/Time

4/15/2020 4:27:08 PM

Recorded Date/Time

4/15/2020 4:27:09 PM

Artifact type

 KnowledgeC Screen Backlight States

Item ID

52566

EVIDENCE INFORMATION

Source

13-4-1.tar\Volumes\JOSH
\NoTar-13-4-1\private\var\mobile
\Library\CoreDuet\Knowledge
\knowledgeC.db

Recovery method

Parsing

Deleted source

Location


Table: ZOBJECT(Z_PK: 20868)

Evidence number

13-4-1.tar

This track being played at 4:17-4:20pm on apple music

com.apple.Music



13-4-1.tar

DETAILS

⌵

ARTIFACT INFORMATION

Application Name

com.apple.Music

Album

Will Smith: Greatest Hits

Title

Summertime

Artist

DJ Jazzy Jeff & The Fresh Prince

Duration (Seconds)

270


Start Date/Time

4/15/2020 4:17:55 PM

End Date/Time

4/15/2020 4:20:15 PM

Artifact type

 KnowledgeC Media History

Item ID

59324

EVIDENCE INFORMATION

Source

13-4-1.tar\Volumes\JOSH
\NoTar-13-4-1\private\var\mobile
\Library\CoreDuet\Knowledge
\knowledgeC.db

Recovery method

Parsing

Deleted source

Location

Table: ZOBJECT(Z_PK: 20843)

At 4:22pm the device was detected at this parked car location:

AXIOM Training

Content types

Apr 15, 2020 - Apr 15,...

Tags and comments

Profiles

Partial results

Keyword lists

CLEAR FILTERS

Type a search term...

GO

ADVA

categorization

Media attributes (VICS)

MATCHING RESULTS (30 of 5,425)

Column view

Item ID	Item	Artifact type	Artifact ca...	Date and time
24159	Local User <13-4-1.tar>	iOS iMessage/SMS/M...	Communication	4/15/2020 4:20:41 PM
24411	Local User <13-4-1.tar>	iOS iMessage/SMS/M...	Communication	4/15/2020 4:20:41 PM
34121	4/15/2020 4:22:54 PM	Parked Car Locations	Location & Travel	4/15/2020 4:22:54 PM
41157	+19195790479	InteractionC Contacts	Application Usage	4/12/2020 4:14:27 PM
41170	auth@getkeepsafe.com	InteractionC Contacts	Application Usage	4/15/2020 4:17:35 PM
41174	+1 (919) 579-0479	InteractionC Contacts	Application Usage	4/15/2020 4:20:42 PM
47198	com.apple.MobileSMS	KnowledgeC Applicati...	Application Usage	4/15/2020 4:21:40 PM
49711	Locked	KnowledgeC Device L...	Application Usage	4/15/2020 4:27:09 PM
49714	Unlocked	KnowledgeC Device L...	Application Usage	4/15/2020 4:16:13 PM
49715	Locked	KnowledgeC Device L...	Application Usage	4/15/2020 1:18:18 AM
51787	Unplugged	KnowledgeC Device P...	Application Usage	4/15/2020 4:22:53 PM
51789	Plugged in	KnowledgeC Device P...	Application Usage	4/15/2020 4:16:15 PM
51790	Plugged in	KnowledgeC Device P...	Application Usage	4/15/2020 4:16:14 PM
51793	Plugged in	KnowledgeC Device P...	Application Usage	4/15/2020 4:16:07 PM
51795	Unplugged	KnowledgeC Device P...	Application Usage	4/15/2020 10:54:53 AM
52563	Screen off	KnowledgeC Screen B...	Application Usage	4/15/2020 4:27:08 PM
52566	Screen on	KnowledgeC Screen B...	Application Usage	4/15/2020 4:16:00 PM
52568	Screen off	KnowledgeC Screen B...	Application Usage	4/15/2020 4:15:48 PM
52572	Screen on	KnowledgeC Screen B...	Application Usage	4/15/2020 4:15:44 PM
52574	Screen off	KnowledgeC Screen B...	Application Usage	4/15/2020 2:52:40 PM
59320	com.apple.Music	KnowledgeC Media H...	Application Usage	4/15/2020 4:22:54 PM

4/15/2020 4:22:54 PM

13-4-1.tar

WORLD MAP PREVIEW

DETAILS

ARTIFACT INFORMATION

Timestamp Date/Time4/15/2020 4:22:54 PM

Latitude35.6594399706748

Longitude-78.8725686083705

Artifact typeParked Car Locations

Item ID34121

EVIDENCE INFORMATION

Source13-4-1.tar\Volumes\JOSH
\\NoTar-13-4-1\private\var\mobile
\\Library\Caches\com.apple.routined
\\Local.sqlite

Recovery methodParsing

Deleted source

LocationTable: ZRTVEHICLEEVENTHISTORYMO
(Z_PK: 73)

Evidence number13-4-1.tar

Outgoing call to this number at 4:20pm

+19195790479

13-4-1.tar

DETAILS

ARTIFACT INFORMATION

Identifier

+19195790479

Display Name

Josh Hickman

Created Date/Time

4/12/2020 4:14:27 PM

First Incoming Interaction Date/Time

4/12/2020 4:14:26 PM

Last Incoming Interaction Date/Time

4/12/2020 4:16:15 PM

First Outgoing Interaction Date/Time

4/15/2020 4:20:41 PM

Last Outgoing Interaction Date/Time

4/15/2020 4:20:41 PM


Incoming Interaction Count

2

Outgoing Interaction Count

1

Artifact type

 InteractionC Contacts

Item ID

41157

EVIDENCE INFORMATION

Source

13-4-1.tar\Volumes
JOSH\NoTar-13-4-1
\private\var\mobile
\Library\CoreDuet
\People
\interactionC.db

1. What specific piece of evidence do you think led the investigators to Billigan's residence?

“After searching Dunslap's home, investigators discovered communications between him a person who was going by the alias of “Lloyd Llewelyn”, but who was later identified as Theodore Billigan. Using a standard legal process, they were able to execute a search warrant on Billigan's residence in Massachusetts, which had IP address 143.244.47.90”

Since they traced the home using IP address, it indicates that the mode of communication had been over the internet.

It could have been that they found chat between Dunslap and Billigan on a private internet forum discussing about rates of Lllamas (obviously using an alias) or about the status of trading another one.

But whatever the platform of communication was, it was able to link Billigan to his IP address (means possible that it wasn't Tor or similar services)

2. What type of legal order do you expect was used by investigators to go from that specific piece of information to an actual street address, and what are the legal requirements and thresholds that must be met in order to obtain and use that legal order?

They had the IP address

Needed: street address

Legal process: subpoena the Internet Service provider requesting subscriber information related to that IP address.

Requirements:

The legal threshold for issuing a subpoena is extremely low. To put it one way, it just has to be information related to an on-going investigation – in this case illegal ring of Lllamas trade.