

OFFENSE - DEFENSE: Advanced Investigations

Scott Schultz
National Account Manager
DigStream Investigations

Garrett McKen
Partner
DigStream Investigations

1

DigStream

"THE INTs"

OSINT



GEOINT



SIGINT



HUMINT



MASINT



2

DigStream

INVESTIGATIVE BREADTH



3

DigStream

"THE INTs"

OSINT



GEOINT



SIGINT



HUMINT



4

DigiStream CROWD-SOURCED INTELLIGENCE

Sociologists have been studying the effects of social media on society and have coined the term "self-surveillance" or "participatory surveillance" to encapsulate a widely-observed phenomenon.

For many people, the desire to promote their "personal brand" is greater than their desire for privacy.

Self-surveillance dominates the social habits of younger generations of "Digital Natives." However, increasingly older generations are the most notable content posters.



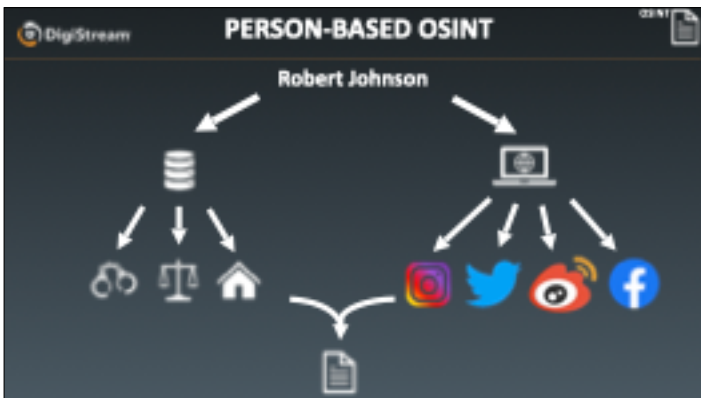
5

DigiStream SURVEY

How often do you use social media?

- A. On a daily basis
- B. Once a week
- C. Rarely
- D. Never

6



7

DigiStream THREE PILLARS OF OSINT

IDENTITY RESOLUTION



GEOGRAPHIC RESOLUTION




CHRONOLOGIC RESOLUTION



8

DigiStream IDENTITY RESOLUTION CASE STUDY 02/91



- 28 year-old trucker claimed a workers' compensation injury due to an alleged cumulative back injury.
- The subject was found to have an active lifestyle on social media.
- An Instagram account was located via a cell number and featured dozens of videos posted by the subject featuring him engaging in skydiving after the date of loss.

9



10

DigiStream THE PROCESS OF IDENTITY RESOLUTION 02/91



11

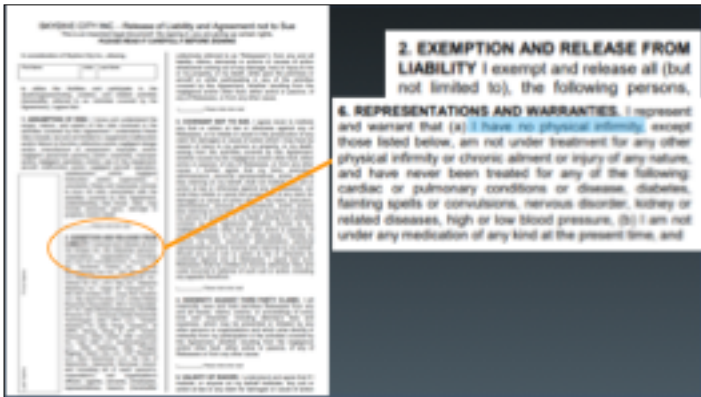
DigiStream THE PROCESS OF GEOGRAPHIC RESOLUTION 02/91



12



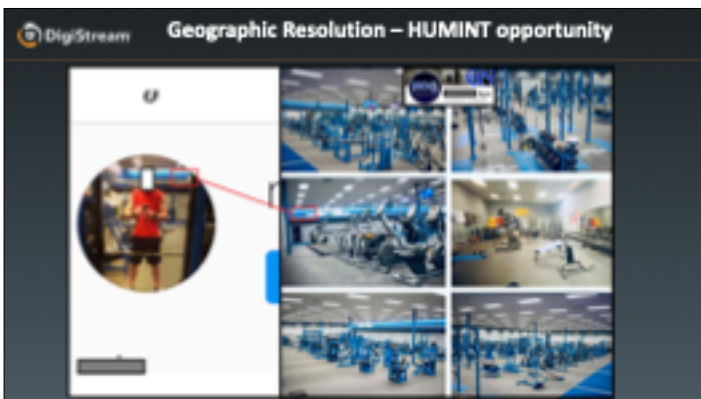
13



14



15



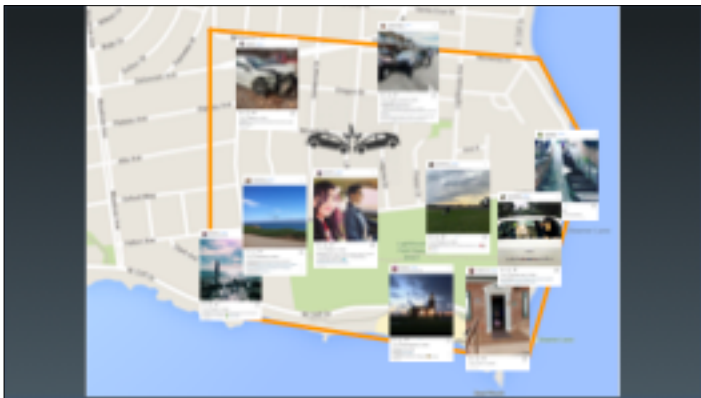
16



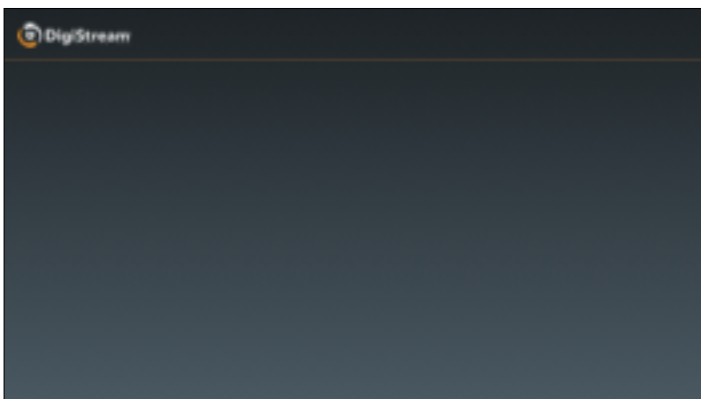
17



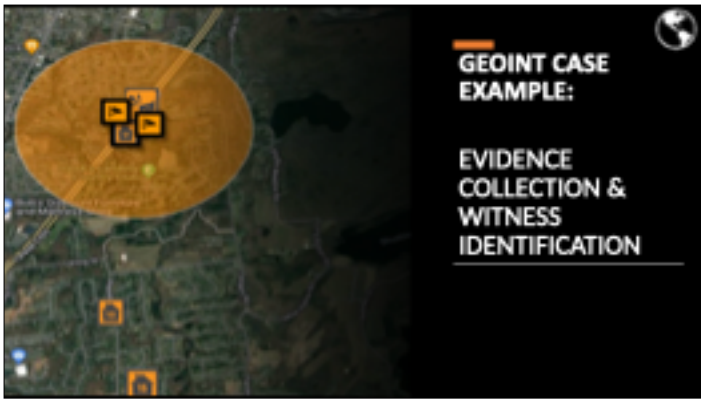
18



19



20



21



22



23

Persons/Locations of Interest						
Possible Witnesses						
Party #	Name/Handle	Photo	Role	Address and Distance from Incident	Contact Information	Link to Post
1	[REDACTED]	[REDACTED]	Possible Secondary Witness "yes he was associated only before I got there"	[REDACTED] 10.9 miles	[REDACTED] [REDACTED]@GMAIL.COM	[REDACTED]
2	[REDACTED]	[REDACTED]	Possible Secondary Witness "Was just there they are using jans of life to get"	[REDACTED] 39.3 miles	[REDACTED] [REDACTED]@GMAIL.COM	[REDACTED]

24

DigiStream GEOINT

3			Possible Secondary Witness "Up in lobby waiting for person"					
4			Possible Secondary Witness Uploaded photo of incident	10.0 miles				
5			Spouse of possible secondary witness "Last I heard right after it happened, he was driving by"	0.0 miles				

25

DigiStream GEOINT

6			Possible Secondary Witness	0.0 miles				
7			Possible secondary witness "I got into my car at 10:15 and saw the car in the lobby. The car was driving towards the entrance of the building. I saw the car and the person who was in the car. I saw the car and the person who was in the car. I saw the car and the person who was in the car."	10.7 miles				
8			Possible secondary witness "I was in the car"	0.0 miles				

26

DigiStream GEOINT

12			Possible Secondary Witness Uploaded photo of incident	20.0 miles				
13			Possible Secondary Witness "I passed by this and all I could see was grey"	44.1 miles				
14			Possible Eyewitness "I got in my car and saw the car. I saw the car and the person who was in the car. I saw the car and the person who was in the car. I saw the car and the person who was in the car."	11.7 miles				

27

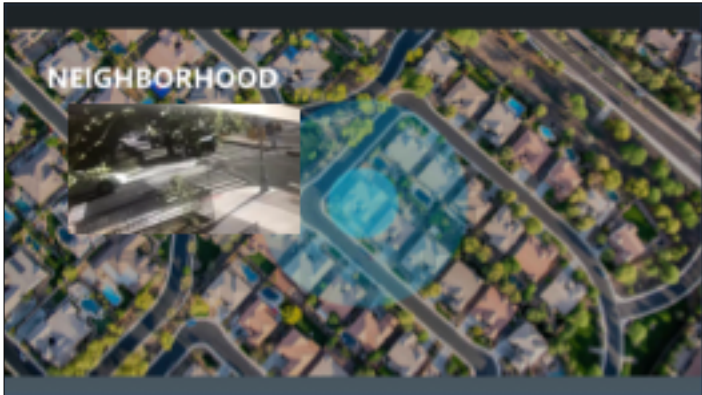
DigiStream GEOINT

Camera Location	Photo	Distance from Incident	Notes
Entrance of [Redacted]		200 ft	Possible to view of the incident
Entrance of [Redacted]		200 ft	Possible to view of the incident
Entrance of [Redacted]		100 ft	Possible to view of the incident

28



29



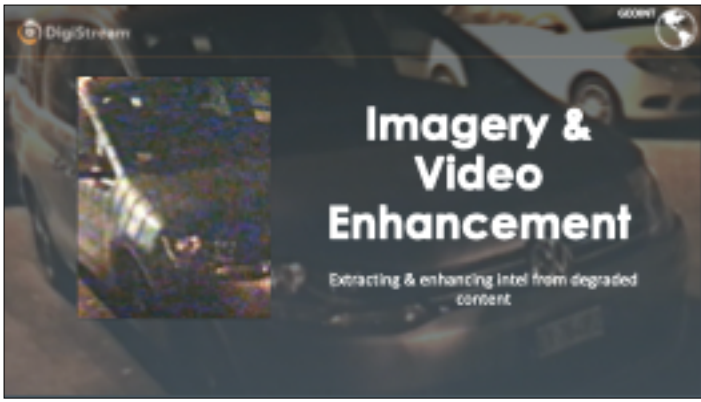
30



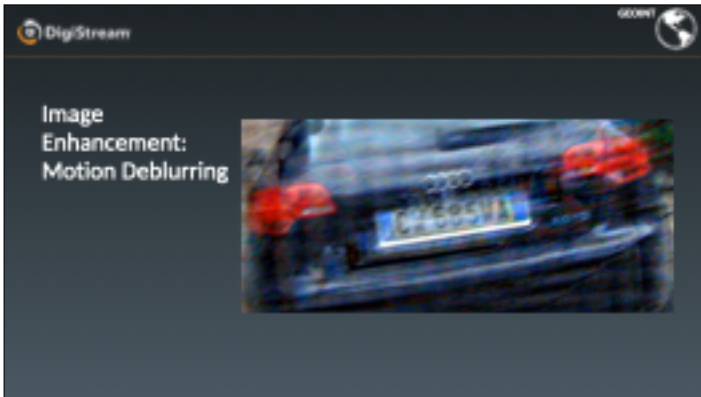
31



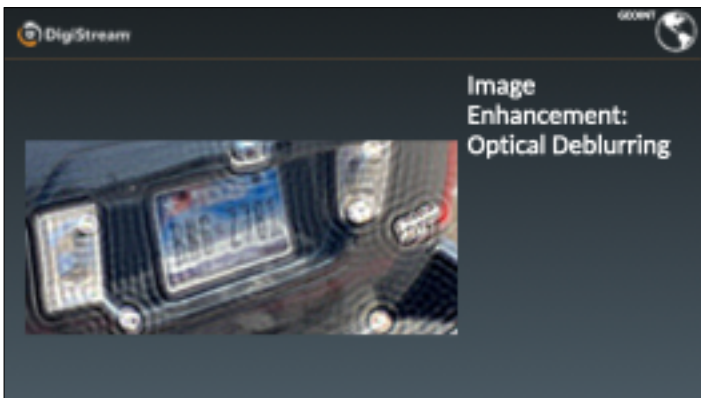
32



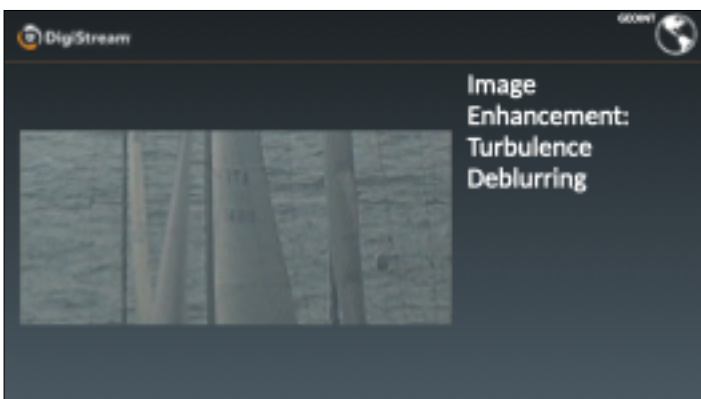
33



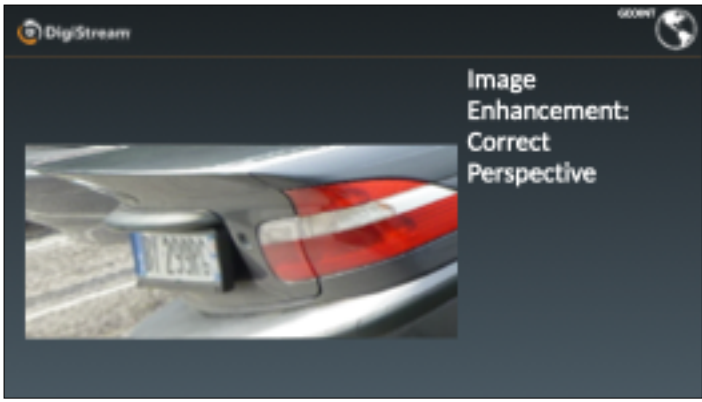
34



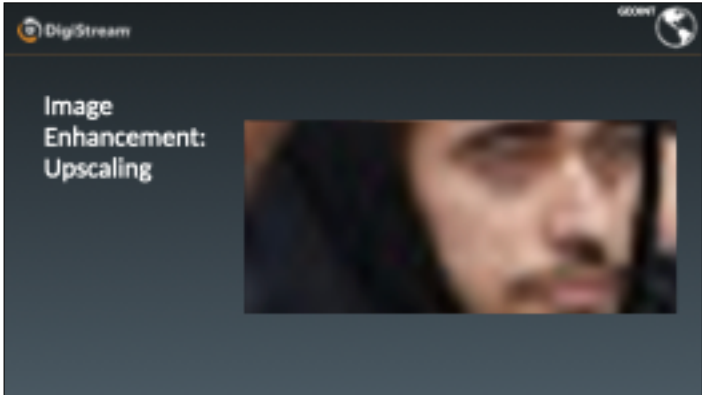
35



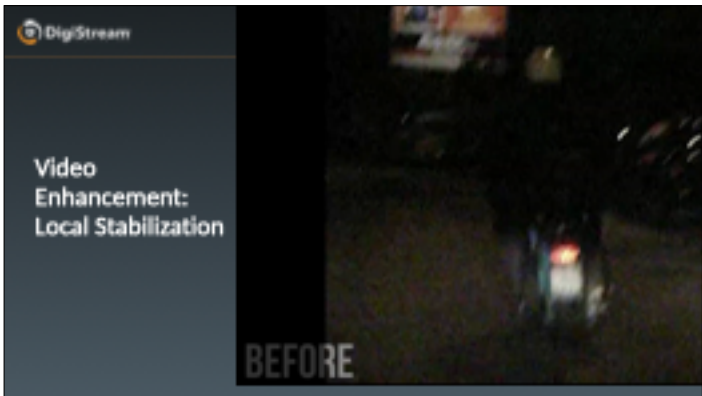
36



37



38



39



40

DigiStream VEHICLE SIGHTING REPORTS

What are they?

- It provides a list of times, dates, and locations where the vehicle has been spotted. Vehicle Sighting data is gathered nationwide at a rate of 220 million each month.

What are some investigative red-flags?

- I. Surveillance efforts do not see the subject or their vehicles at the residence.
- II. Background Records uncover multiple addresses within a year.
- III. There is a hunch the subject is engaged in outside employment.

41

DigiStream VEHICLE SIGHTING REPORTS

Automated License Plate Recognition

42

DigiStream VEHICLE SIGHTING REPORTS

LIVE SIGHTING ALERT

➤ You can tailor your searches by receiving live notification alerts when the subject's vehicle has been spotted.

How To Utilize Live Sighting Alerts?

- **Challenging cases with no activity.**
A live alert can re-energize the investigation by increasing the new lead opportunity.
- **Challenging cases with limited activity.**
By authorizing a reserve spot-check, a live alert can steer into a full day of prime opportunity.

43

DigiStream Vehicle Sighting Analytics

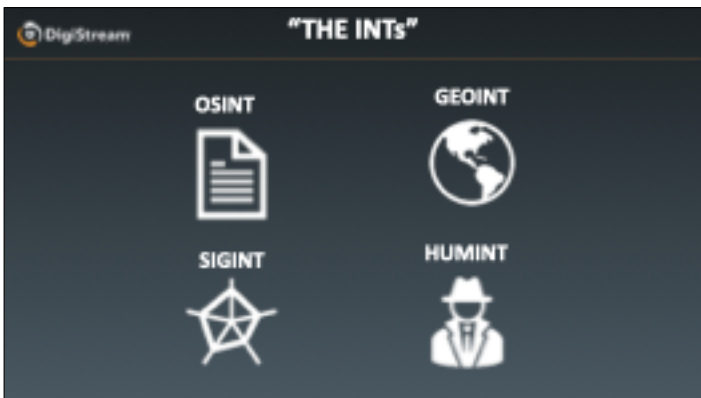
44



45



46



47



48

49

SCOPE
Mobile Phone Capabilities:

- Device state (face-up/face-down)
- Text logs
- Call logs
- App data
- Location data
- Health data
- Photo/Video metadata
- Private chat data
- Deleted Data

50

SCOPE

In addition to mobile phones, any device with memory storage can be analyzed and the extracted data examined to find key pieces of evidence such as:

- Documents or texts (with metadata)
- Videos and photographs
- Location data
- Health data and more

51

COMMON DEVICE REQUESTS

<p>Mobile Phones Individual phone device, as well as within apps and the cloud may be extracted along with information about the state of the device at specific times/date.</p>	<p>Personal Computers Files, folders, transactions and logs can be examined, as well as "deleted" content.</p>
<p>Internet of Things (IoT) A broadly specified term for any device that stores data locally in some cases, device data is not remotely hosted, downloaded or uploaded.</p>	<p>Vehicle Black Box Computers within motor vehicles, capture a wealth of data including speed, acceleration, runtime, and diagnostic codes.</p>

52

OBTAINING EVIDENCE

IDENTIFY THE OPPORTUNITY
Parties to the suit may utilize components about devices that store information pertinent to the investigation.

INTERROGATORIES & DEPOSITIONS
Knowing what type of information will be retained under specific forms of that data will aid a party's process interrogations. We know where the relevant information is stored.

KNOW THE PROCESS
In most cases, devices will need to be transferred, using chain of custody procedures. Device turnaround is typically 3-5 business days.



53

PROCESS



DEVICE RECEIVED

Mobile devices are often shipped to S&NT even using chain-of-custody measures. Device examinations available for legal proceeds.



DATA IMAGING

All data stored on the device is retrieved and stored electronically for analysis using industry centered technology.



DEVICE RETURNED

As soon as the data retrieval is complete and checked for accuracy the device is returned to the client/owner.



DATA ANALYSIS

Obtained data is analyzed and reports compiled that clearly identify the scope of the investigation and results.



REPORTING

Case-relevant data is identified and included in a written report to clearly summarize the most notable investigative findings.



54

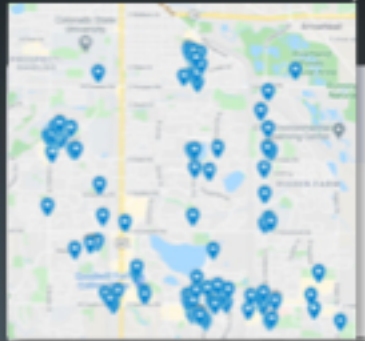
CASE STUDIES



55

MOBILE PHONE

- Background: Subject allegedly contracted COVID-19 at work. We were asked to investigate his phone to trace his movements and activities leading up to his diagnosis.
- Forensics revealed emails suggesting involvement in community social events, and GPS data placed the device near addresses associated with these events.





56

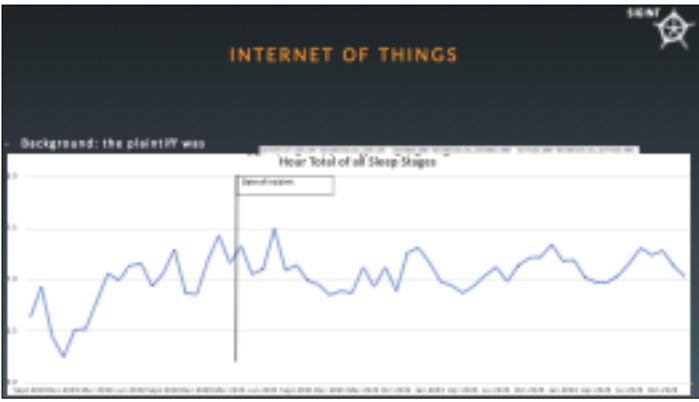
MOBILE PHONE

- Background: Subject driving a commercial truck ran a stop sign, killing a young woman in another vehicle.
- Forensics revealed that at the time of the incident, the subject's cell phone was playing a continuous stream of Snapchat videos, many of which contained adult content.



The accident occurred at 11:30am

On 10/26/2020 at 11:30am, [redacted] was driving a commercial truck at the intersection of [redacted] and [redacted] when he ran a stop sign and struck a young woman in another vehicle, killing her.



57

INTERNET OF THINGS

SIGINT 

SUMMARY

A competent attorney must recognize when data collected from mobile devices, computers, and IoT may be useful in their case. Sample interrogatories are available, as well as a one-page affidavit that can be used in court to obtain subpoenas. Questions can be directed to bigint@i4m.com and one of our technical experts can guide you through the process.

58



59



60

61

LIMITATIONS OF SINGLE-HANDED SURVEILLANCE

Use of a single Investigator is often seen as a necessity on most cases, but there are inherent disadvantages to consider:

- The solo Investigator must be able to see the subject's residence – opening themselves to suspicion





64

LIMITATIONS OF SINGLE-HANDED SURVEILLANCE

Use of a single Investigator is often seen as a necessity on most cases, but there are inherent disadvantages to consider:

- The solo Investigator must be able to see the subject's residence – opening themselves to suspicion
- A solo Investigator risks losing a subject who uses an alternate exit from the residence



65

Limitations of Single-Handed Surveillance

Use of a single investigator is often seen as a necessity on most cases, but there are inherent disadvantages to consider:

- The solo investigator must be able to see the subject's residence – opening themselves to suspicion
- A solo investigator risks losing a subject who uses an alternate exit from the residence
- A solo investigator must always follow the subject, or risk losing them

66



67

Limitations of Single-Handed Surveillance

Use of a single investigator is often seen as a necessity on most cases, but there are inherent disadvantages to consider:

- The solo investigator must be able to see the subject's residence – opening themselves to suspicion
- A solo investigator risks losing a subject who uses an alternate exit from the residence
- A solo investigator must always follow the subject, or risk losing them
- A bad intersection can derail a solo investigator and lead to a loss

68



69

LIMITATIONS OF SINGLE-HANDED SURVEILLANCE

Use of a single investigator is often seen as a necessity on most cases, but there are inherent disadvantages to consider:

- The solo investigator must be able to see the subject's residence – opening themselves to suspicion
- A solo investigator risks losing a subject who uses an alternate exit from the residence
- A solo investigator must always follow the subject, or risk losing them
- A bad intersection can derail a solo investigator and lead to a loss
- A solo investigator may lose sight of the subject when transitioning from a vehicle follow to a foot follow, and vice versa

70



71

ADVANCED SURVEILLANCE

Conducting better surveillance on fewer people creates a healthy industry dynamic

- Use of remote cameras mitigates the subject's suspicion in and around their residence

72




73

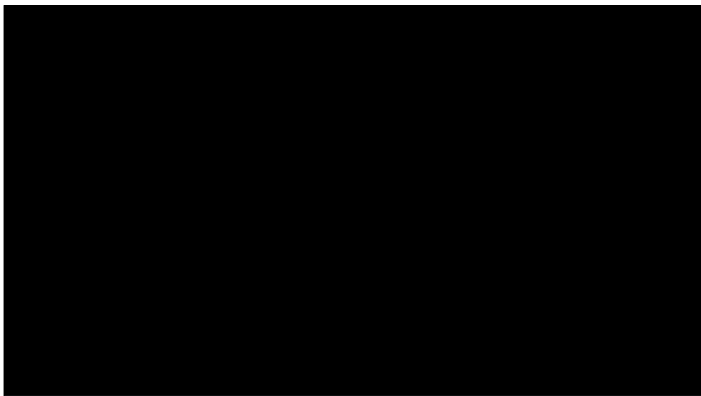
DigiStream **ADVANCED SURVEILLANCE** HELMINT

Conducting better surveillance on fewer people creates a healthy industry dynamic

- Use of remote cameras mitigates the subject's suspicion in and around their residence
- Remote cameras allow for long-range setups in rural environments or in environments with "wise" subjects.



74




75

DigiStream **ADVANCED SURVEILLANCE** HELMINT

Conducting better surveillance on fewer people creates a healthy industry dynamic

- Use of remote cameras mitigates the subject's suspicion in and around their residence
- Remote cameras allow for long-range setups in rural environments or in environments with "wise" subjects.
- Multi-crew investigations allow for rotating tails and a much wider search area in the rare event of a loss



76



77



78

DigiStream **ADVANCED SURVEILLANCE** PLANNING

Multi-Crew

- Multiple investigators allows for one to watch the residence and another to perform the actual pick-up
- Multiple investigators reduces the need for "buffer cars" in certain situations and allows for smooth hand-offs. This further limits suspicion during vehicular follows
- In the event of a loss, the surveillance team can search in multiple directions instead of just one



79

DigiStream **ADVANCED SURVEILLANCE** PLANNING

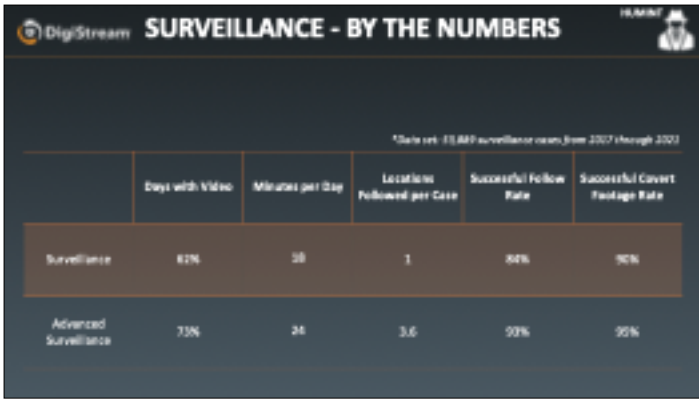
Deploying advanced surveillance on your case limits risk in the most important area - the subject's home. However, aware subjects pose significant risk during follows.

The following scenarios may warrant multi-crew (or remote camera enhanced) surveillance teams to delay suspicion:

- Case involves a law enforcement officer, or a well-informed union member
- Subject resides in a high-rise apartment complex with multiple exit/entry points
- Subject resides in a rural environment
- Subject has "made" other investigators previously



80



81



82

THANK YOU FOR YOUR KIND ATTENTION

Scott Schultz
National Account Manager
DigiStream Investigations

Garrett McGinn
Partner
DigiStream Investigations

Questions?

www.digistream.com
www.digistream.com/press

83
