

Did the FBI Hack Bitcoin? Deconstructing the Colonial Pipeline Ransom

Author: Tuan Phan, Founder, Zero Friction LLC

Date Published: 1 July 2021

On 7 May, 2021, Colonial Pipeline, a US oil pipeline system, that mainly carries gasoline and jet fuel to the southeastern United States suffered a ransomware cyberattack that impacted the computerized equipment that managed the pipeline. The company learned of the attack shortly before 5 a.m. when an employee discovered a ransom note on a system in the IT network. The company believes that the attack was orchestrated by [DarkSide](#), a cybercriminal group believed to operate, at least in part, out of Russia.

On 13 May, the general public learned that Colonial Pipeline paid approximately 75 Bitcoins, or around US\$5M, in ransom. Criminal organizations such as DarkSide prefer the use of Bitcoin as ransom payment because it provides a degree of anonymity, allows for the transfer from one person to another without the use of a bank, and lastly, can be converted back into fiat via multiple methods, some of which do not require the use of a legal name or address.

On 7 June, the US Federal Bureau of Investigation (FBI) announced that it recovered nearly \$2.3M of the stolen funds using money flow analysis and other investigative techniques. Coinciding with the China crackdown on Bitcoin mining, the news of the FBI's "hack" of Bitcoin sent the broader market for cryptocurrencies tumbling. While the FBI did not provide specific details of the recovery process in order to safeguard their methods for future investigations, the seizure warrant filed with the US District Court, Northern District of California, did provide some insights.

The public gained additional details of the event the next day as Colonial Pipeline CEO Joseph Blount Jr., recalled the event to members of the Senate Homeland Security and Governmental Affairs Committee in prepared remarks. Specifically, company personnel received a ransom note on its network stating that the hackers had "exfiltrated" material from the company's shared internal drive and demanded approximately \$5 million in exchange for the files. Immediately following the discovery, Colonial Pipeline commenced the process to shut down the entire pipeline to minimize further risks from the malware to the Operational Technology (OT) network that controls Colonial's pipeline operations. The shutdown caused major disruptions to fuel delivery up and down the East Coast, airline transportation, as well as consumer fuel distribution, which immediately resulted in long lines at pumps throughout the Southeastern U.S.

In this blog post, I will attempt to reconstruct the recovery process for the readers. It is important to note that neither the author nor the company, Zero Friction, has access to any nonpublic information about this event. All methods and techniques discussed were obtained using Zero Friction's expertise and publicly available open-source intelligence (OSINT) tools.

According to the FBI’s [seizure warrant](#), the FBI has performed a money flow analysis using onchain Bitcoin data. However, the FBI obfuscated most of the addresses of interest, specifically:

- 1. DarkSide’s ransom payment address
- 2. Intermediate addresses where DarkSide transferred the ransom payment
- 3. The DarkSide collection address from which the FBI seized the partial ransom payment (this is referred to as the Subject Address in the seizure warrant)
- 4. The FBI’s holding address where the seized funds are currently being held

Starting with the partial address provided by the FBI, shown in the image below, the author constructed a query to search the Bitcoin network for all addresses that partially match the address. The same technique utilized can also be applied to other use cases on other blockchain platforms, including Ethereum, to search for specific transaction value, type of transaction periods of time, and others.


33. An online public blockchain explorer identified at least 23 other addresses collected together with address XXXXXXXXXXXXXuRTnHQA8tNuG7S2pKcdNx¹B in one wallet. [REDACTED] on May 27, 2021, funds from the collection of addresses, totaling 69.60422177 BTC, including 63.70000000 BTC accessible from address XXXXXXXXXXXXXuRTnHQA8tNuG7S2pKcdNx¹B was transferred to address XXXXXXXXXXXXX950klpj²cawuy4uj39ym43hs6cfsegq (the “Subject Address”), and it has not moved since.

34. The private key for the Subject Address is in the possession of the FBI in the Northern District of California.

For the Colonial Pipeline case, the query returns only one result, and by comparing to the returned information, the author concluded with a high degree of certainty that the result is the Subject Address (Item #3):

Row	addresses	value	block_timestamp
1	bc1qq2euq8pw950klpj ² cawuy4uj39ym43hs6cfsegq	590422177	2021-06-07 17:45:41 UTC

Using a Bitcoin explorer (e.g., [blockchair.com](#)), the author was able to determine that the address has a total of three transactions (one deposit received and two transfers sent), with the earliest transaction shown as “received.”



Address
**bc1qq2euq8pw950klpjcauwuy4uj39ym43hs6cfs
egq**

Balance

0 BTC · 0 USD


Total received

75.50844354 BTC · 2,890,589.80 USD

Total spent

75.50844354 BTC · 2,704,259.30 USD

Transaction history

 Sent


5.90422177 BTC · 211,454.00 USD

Transaction: 280c546369

Confirmed

Jun 7, 2021 5:53 PM UTC

Senders: 1 Recipients: 1

 Sent


63.70000000 BTC · 2,281,356.00 USD

Transaction: 943f24cf7a

Confirmed

Jun 7, 2021 5:45 PM UTC

Senders: 1 Recipients: 2

 Received

69.60422177 BTC · 2,679,140.00 USD

Transaction: daf38e69d9

Confirmed

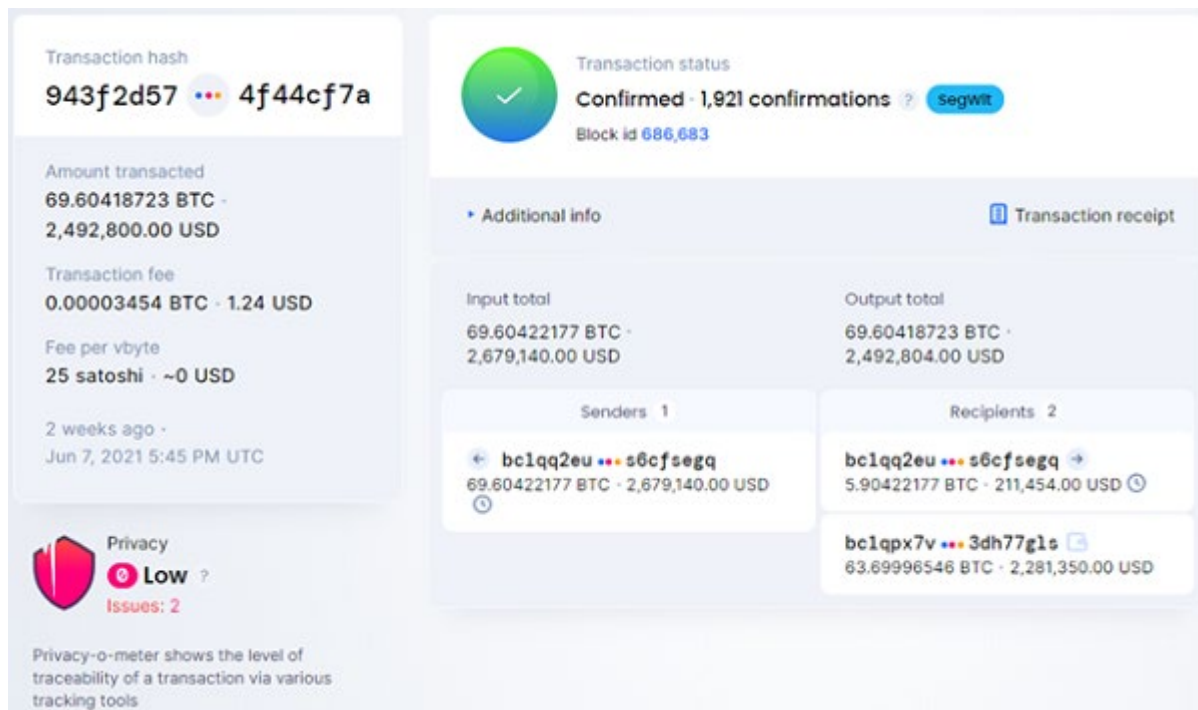
May 28, 2021 3:06 AM UTC

Senders: 24 Recipients: 1

Since seizures typically require taking custody of the fund in the seized address, it is expected to observe a transaction that moves the seized fund into an address controlled by the law enforcement entity. This action is necessary to mitigate any chance that the hacker(s) has access to a backup set of the same private keys and attempt to move the fund before the seizure can be fully completed. Accordingly, the first transaction hash:

943f2d576ed8d9f388ba75eb82fe35cce29479b84121827ac368a5a94f44cf7a

highlighted the described action in which approximately 63.7 BTC was moved to an address `bc1qpx7vyv5tp7dm0g475ev527krq764t73dh77gls`, identified as the FBI's holding address (Item #4), where it remains unspent as of today.



The transaction has the following properties:

1. Only one input (e.g. sender) and two outputs (e.g. recipients)
2. The input address was reused as the change address

This transaction pattern significantly reduces the anonymity of addresses, allowing the author to conclude that the two addresses likely belong to two different wallets, and are controlled by different parties. This observation can also be confirmed by performing a clustering analysis where neither address is related to any other addresses with prior transactions on the network (e.g., part of the same wallet).

Approximately eight minutes after the transfer of the 63.7 BTC into the FBI's address, the remaining balance was moved by a second transaction hash

280c5f96397b9502b99703842712b78fda84f1a0faabf826f683448082f46369

to address bc1qvjh9cq6qlj4f4q5vxnkgt25mc6qlld04vv20fhe, where it remains unspent as of today.

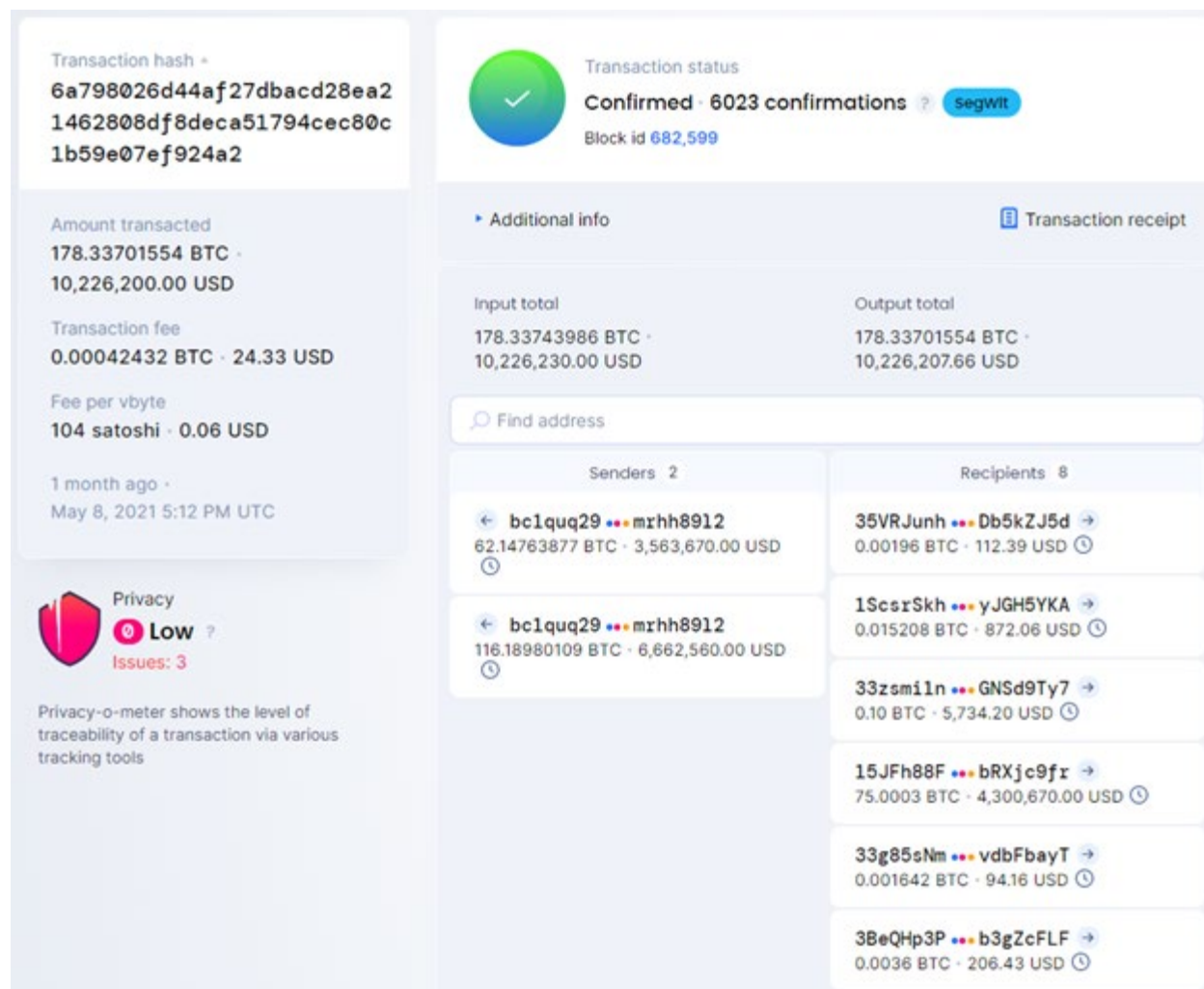
Why did the FBI not seize the entire balance of the subject address since the available total of 69.6 BTC total was well within the 75 BTC paid for the ransom? To answer this question, it is necessary to conduct a money flow for the transaction back to the initial ransom payment.

Starting with the subject address, a backward trace was performed by following the larger inbound inputs. Five hops later across several intermediate addresses (Item #2), the trace concludes at address 15JFh88FcE4WL6qeMLgX5VEAFcBRXjc9fr also confirmed by the FBI as the DarkSide ransom payment address (Item #1).

28. On or about May 8, 2021, Victim X advised the FBI that it was instructed to send a ransom payment of approximately 75 BTC, calculated to be worth approximately \$4.3 million on that date, to cryptocurrency address XXXXXXXXXXXXXL6qeMLgX5VFAFCbRXjc9fr.

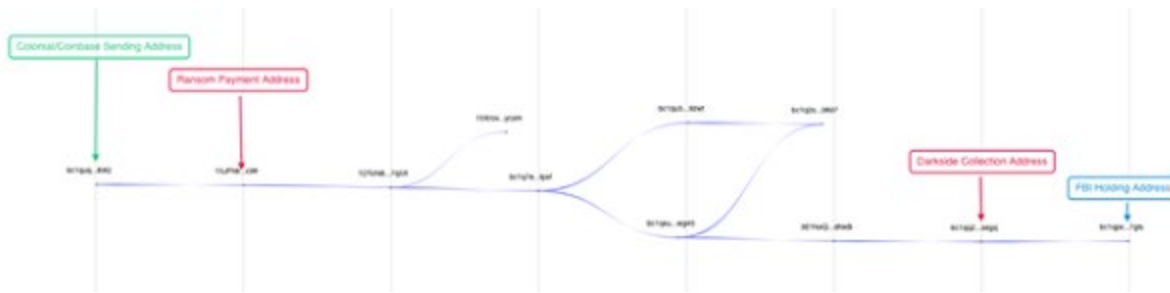
Furthermore, by taking one additional hop back from the ransom payment address, the author was able to determine that Colonial made the payment on 8 May 2021 at 5:12 PM UTC via Coinbase's sending address, bc1quq29mutxkgxmjdr7ayj3zd9ad0ld5mrhh89l2, with the corresponding transaction hash

6a798026d44af27dbacd28ea21462808df8deca51794cec80c1b59e07ef924a2



Source: FBI's Seizure Warrant

The complete picture of the Colonial Pipeline ransom event can be visualized, as shown below, through the use of a blockchain forensic solution, such as Breadcrumbs.app, where the thickness of the lines between addresses is weighted to the transaction values exchange. A larger view of the same image may be viewed [here](#).

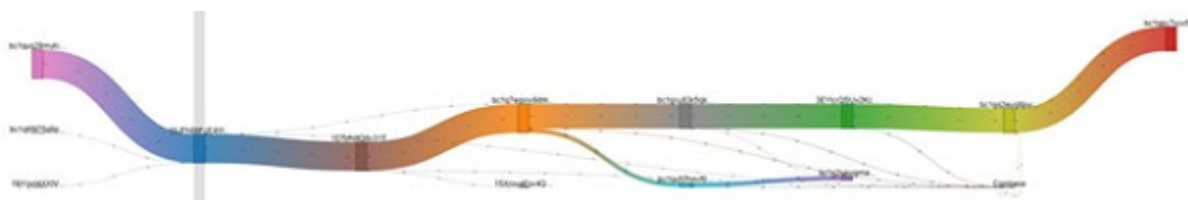


Forensic solutions offer a key advantage over OSINT solutions by providing curated and ongoing updates to address attribution to known hackers and users, and services such as exchanges, mixers, etc. The usage of blockchain forensic solutions also improves the quality of forensic investigations and significantly reduces the time to conduct them.

Key transactions mapped to the above transaction graph are:

Transaction Hash	Description
6a798026d44af27dbacd28ea21462808df8deca51794cec80c1b59e07ef924a2	Ransom payment (Item #1)
915fb4f0a030937f2c1d2210996e8eb32b5a41b331965c7ec78961923775bd62	Intermediate #1
fc78327d4e46dac01dc313067b1ac7f274cdb3a07ea9f28f6f71473145f1b264	Intermediate #2
0677781a5079eae8e5cbd5e6d9dcc5c02da45351a3638b85c88e5e3ecdc105a7	Intermediate #3
9436dbf0435b15378f309c35754a110db880fa9bb66a062160a25533bb4a212a	Intermediate #4
daf38c7b38eb0a587cf843f47000d5c294affb4f56017370ad48c5147f5e69d9	Sent to Subject Address (Item #3)
943f2d576ed8d9f388ba75eb82fe35cce29479b84121827ac368a5a94f44cf7a	Sent to FBI 's Holding Address (Item #4)

In addition, the Sankey diagram can be constructed to track the money flow from the Colonial/Coinbase sending address to the FBI holding address, with the DarkSide ransom payment address highlighted indicated with a gray vertical line. Money flow analysis reduces the complexity of blockchain analysis by focusing on only the large movement of funds starting from a given address. A larger viewable Sankey diagram can also be downloaded from the [following URL](#).

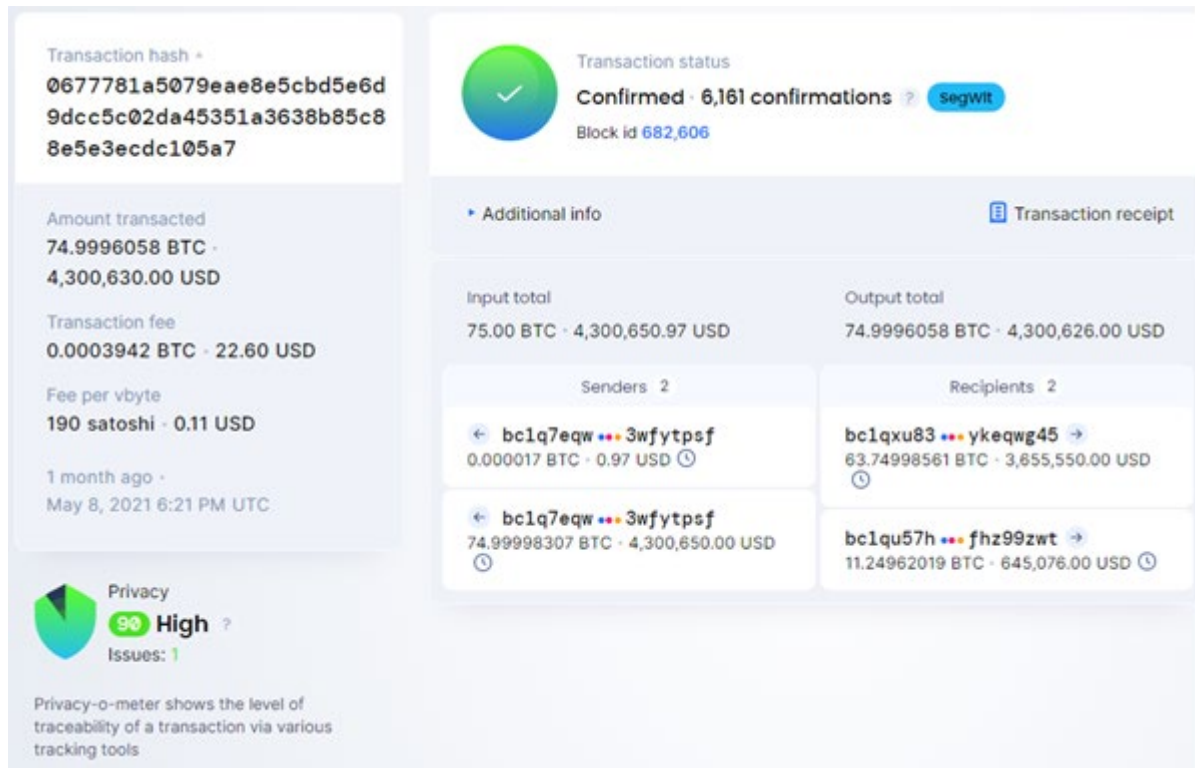


It is important to state that the “Coinbase” label shown in the Sankey diagram has no relationship to the exchange [Coinbase.com](#) but simply denotes the first transaction in a block. A [Coinbase transaction](#) is a unique type of Bitcoin transaction created by a miner to collect the block reward for their work and any other transaction fees collected by the miner.

The key as to why the FBI only seized 63.7 BTC lies in transaction hash:

0677781a5079eae8e5cbd5e6d9dcc5c02da45351a3638b85c88e5e3ecdc105a7

where, of the 75 BTC sent as a ransom payment, address `bc1qXu83k5qkj8kcqdqenwzn7khw4llfykeqwg45` received only 63.7 BTC, with the balance moved to another address. Since DarkSide operates as a Ransomware as a Service where the affiliates pay the service for the use of the ransom tools, the payment of 63.7 BTC is likely the fees to the affiliate, and the remaining balance is likely the share for the DarkSide developer.



The DarkSide Developer share of 11.2 BTC, or 15% of the 75 BTC paid, was sent to address

`bc1qu57hnxf0c65fsdd5kewcsfeag6sljgfhz99zwt`, and that address further sent (shown below) the BTC into a holding address `bc1q2sewgrnau4e4gvceh8ykzf8lqxawpluu0k0607`

that currently has an unspent balance of 107.8 BTC. The author was able to confirm that the address is the holding address for the DarkSide Developer, by examining the patterns paid into the address as commission payments (e.g., 24 senders shown below) as inputs at transaction hash

`b0e381d02d966acbcd9224817e3db50b2bc3566e0060db36a6a17ee163152dd7`

Clustering analysis of addresses relating to `bc1q2sew...uu0k0607` reveals no other related addresses. The author also postulates, based on observed payment patterns, that the DarkSide developer address is likely to reside within a non-custodial (e.g., offline) wallet controlled by the developer.

Transaction hash

b0e381d02d966acbcd9224817e3db50b2bc3566e0060db36a6a17ee163152dd7

Amount transacted

107.80 BTC · 5,215,690.00 USD

Transaction fee


0.00073666 BTC · 35.64 USD

Fee per vbyte

44 satoshi · 0.02 USD

1 month ago ·

May 13, 2021 6:03 PM UTC




Privacy

Low ?

Issues: 4

Privacy-o-meter shows the level of traceability of a transaction via various tracking tools



Transaction status

Confirmed · 5293 confirmations ?

Block id **683,474**

Additional info

Transaction receipt

Input total

107.80073666 BTC · 5,917,299.10 USD

Output total

107.80 BTC · 5,215,690.00 USD

Find address

Senders 24

bc1q6zy0...pweggsce

0.0253571 BTC · 1,476.14 USD

bc1q6l5f...jznq6sss

0.00293188 BTC · 160.72 USD

bc1qyqzm...sd2df8qp

1.11176522 BTC · 64,720.30 USD

bc1q92aq...4m59pqc1

0.007975 BTC · 382.59 USD

bc1qhcmp...wl8f2c5j

0.00719504 BTC · 394.43 USD

bc1qnaka...5c57lgtr

0.00011042 BTC · 5.90 USD

bc1qnaka...5c57lgtr

0.00011042 BTC · 5.90 USD

Recipients 1

bc1q2sew...uu0k0607

107.80 BTC · 5,215,690.00 USD

The next and probably most speculative question is how the FBI was able to obtain the private keys for the Subject Address as this would require obtaining the node IP address leveraged by the affiliate and then, through legal means, gaining access to the actual host itself that holds the private keys. From Bitcoin mechanics, it is possible to obtain the IP addresses for all Bitcoin nodes by scanning the internet for every host with port 8333 (e.g., the Bitcoin core port). Once known, the hosts can then be monitored in real time, allowing for the identification of the IP address that first transmitted the transaction of interest. Combining such information with an IP locator lookup, details on the location, service provider, type, etc., can be obtained, such as shown in the example below:

IP Details For: 160.178.33.236

Decimal: 2696028652
Hostname: 160.178.33.236
ASN: 36903
ISP: Maroc Telecom
Organization: Maroc Telecom
Services: None detected
Type: [Broadband](#)
Assignment: [Likely Static IP](#)
Continent: Africa
Country: Morocco
State/Region: Fes
City: Fes



Latitude: 34.0368 (34° 2' 12.48" N)

Longitude: -5.0008 (5° 0' 2.88" W)

[CLICK TO CHECK BLACKLIST STATUS](#)

Accordingly, the author postulated that the FBI may utilize similar techniques to identified IP addresses by clustering timestamp and transaction details. Without disclosing the specifics to preserve the integrity of the technique as utilized by the FBI, the author confirmed several US-based IP addresses where transactions of interest could have originated, which the FBI could leverage to further identify the host(s) of the DarkSide hacker.

This blog analysis highlights that, while Bitcoin blockchain can offer a degree of anonymity, it is important to understand that such protection can be unmasked in the hands of a qualified blockchain forensic investigator to gain significant information, relative to what could be known to the public using various investigative tools and techniques. Furthermore, using blockchain forensic solutions such as Breadcrumbs.app, the identity of users or services to specific addresses can also be obtained, allowing for legal means to pursue, including seizure and prosecution. As a result of these advances, the attraction for using Bitcoin as payment for ransom is slowly waning.