

[illegible]

<b>Name</b>	Dumb Assassin
<b>URL</b>	<a href="https://www.attackdefense.com/challengedetails?cid=58">https://www.attackdefense.com/challengedetails?cid=58</a>
<b>Type</b>	Forensics : WiFi

**Important Note:** This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic.

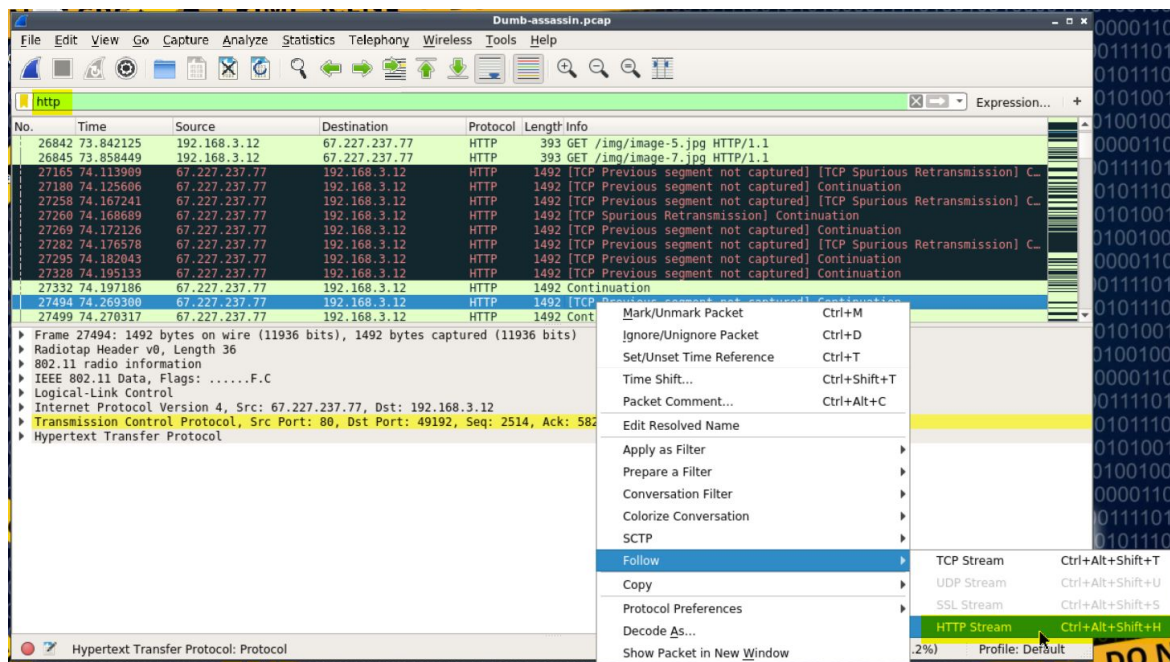
**Question 1:** Who is the target?

**Solution:**

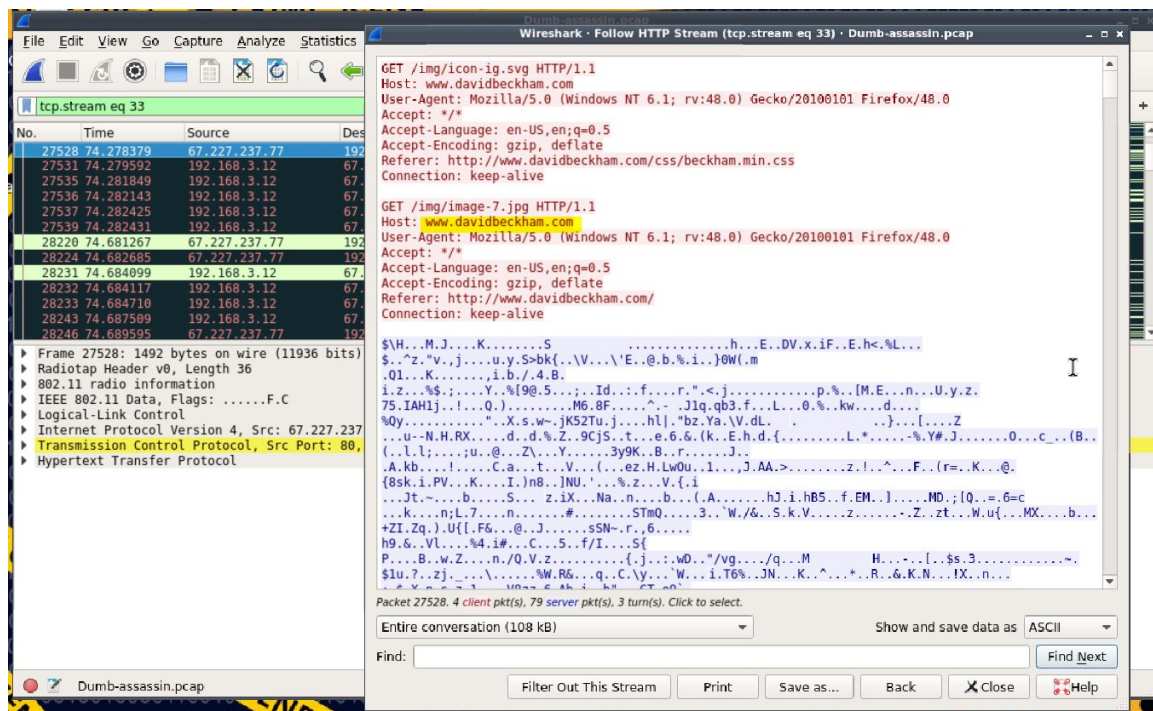
HTTP is the most common way to lookup for the information. And, the objective is to look for the activities focused on gathering information about an individual. If we filter the HTTP traffic.

**Filter:** http

## Check different HTTP streams



## HTTP Stream related to David Beckham's website



Answer: David Beckham

**Question 2:** While analyzing the traffic did you find anything which can help to get an idea of his next plans?

**Solution:**

Similarly, by checking the remaining HTTP traffic, traffic related to other activities can be found.

## Spygadget

The image shows a Wireshark packet capture analysis of a file named 'Dumb-assassin.pcap'. The filter bar at the top is set to 'http.request.method==GET'. The packet list on the left shows several HTTP GET requests. The selected packet (No. 74235) is a GET request to 'http://www.spygeargadgets.com/mini-spy-cameras/'. The packet details pane on the right shows the full request, including the Host, User-Agent, Accept, Accept-Language, Accept-Encoding, Connection, Upgrade-Insecure-Requests, Pragma, and Cache-Control headers. The full request URI is highlighted in blue.

No.	Time	Source	Destination	Protocol	Length	Info
71656	157.199463	192.168.3.12	23.211.195.36	HTTP	1437	GET /places/airports/search?string=New HTTP/1.1
71846	158.036095	192.168.3.12	75.126.75.221	HTTP	836	GET /campaign/rbt/adx/cmradddthis.php?cs_uid=5774c46e1efb7d26 HTTP/1.1
72604	160.991604	192.168.3.12	104.122.76.94	HTTP	980	GET /analyze/utm.html HTTP/1.1
73171	163.868735	192.168.3.12	23.211.195.36	HTTP	1437	GET /places/airports/search?string=Mos HTTP/1.1
73270	164.153726	192.168.3.12	23.211.195.36	HTTP	1438	GET /places/airports/search?string=Mosco HTTP/1.1
73293	164.293655	192.168.3.12	23.211.195.36	HTTP	1439	GET /places/airports/search?string=Mosco HTTP/1.1
73931	168.921291	192.168.3.12	23.211.195.36	HTTP	1467	GET /flights/results/airjson?from=JFK&to=DME&trip_type=OneWay&adult...
74235	170.710862	192.168.3.12	192.200.175.27	HTTP	491	GET /mini-spy-cameras/ HTTP/1.1
74477	171.377720	192.168.3.12	23.211.195.36	HTTP	1514	GET /flights/results/airjson?from=JFK&to=DME&trip_type=OneWay&adult...
74587	171.613061	192.168.3.12	192.200.175.27	HTTP	474	GET /template/menu.css HTTP/1.1
74676	171.820782	192.168.3.12	192.200.175.27	HTTP	485	GET /template/Styles/sgcustom.css HTTP/1.1
74677	171.820935	192.168.3.12	192.200.175.27	HTTP	485	[TCP Fast Retransmission] GET /template/Styles/sgcustom.css HTTP/1.1
74678	171.823805	192.168.3.12	192.200.175.27	HTTP	485	[TCP Fast Retransmission] GET /template/Styles/sgcustom.css HTTP/1.1

Frame 74235: 491 bytes on wire (3928 bits), 491 bytes captured (3928 bits) on interface 0  
Radiotap Header v0, Length 36  
802.11 radio information  
IEEE 802.11 Data, Flags: .....TC  
Logical-Link Control  
Internet Protocol Version 4, Src: 192.168.3.12, Dst: 192.200.175.27  
Transmission Control Protocol, Src Port: 49404, Dst Port: 80, Seq: 1, Ack: 1, Len: 379  
Hypertext Transfer Protocol  
GET /mini-spy-cameras/ HTTP/1.1\r\nHost: www.spygeargadgets.com\r\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; rv:48.0) Gecko/20100101 Firefox/48.0\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8\r\nAccept-Language: en-US,en;q=0.5\r\nAccept-Encoding: gzip, deflate\r\nConnection: keep-alive\r\nUpgrade-Insecure-Requests: 1\r\nPragma: no-cache\r\nCache-Control: no-cache\r\n\r\n[Full request URI: http://www.spygeargadgets.com/mini-spy-cameras/]\r\n[HTTP request 1/9]

Packets: 155548 · Displayed: 510 (0.3%) Profile: Default



## BigCommerce

The image shows a Wireshark packet capture window titled "Dumb-assassin.pcap". The filter bar at the top displays "http.request.method==GET". The packet list on the left shows several HTTP GET requests. The selected packet (No. 74477) is an HTTP GET request to "http://www.cleartrip.com/flights/results/airjson?from=JFK&to=DME&trip\_type=OneWay&adults=1&childs=0&infants=0&ver=V2&type=json&class=Economy&airline=&carrier=&search.v". The packet details pane on the right shows the structure of the request, including the Host, User-Agent, Accept, Accept-Language, Accept-Encoding, X-Requested-With, Referer, and Cookie fields. The Cookie field is truncated and shows "origin=mum; mob=0; Apache=4050a5fc.5375924e85ddb; ak\_bmsc=47584E1EEF38531C863B9C6D25DAEF8717D3874A1C3B0000EF6C8357BEF90304-plv3". The packet bytes pane at the bottom shows the raw data of the request.

No.	Time	Source	Destination	Protocol	Length	Info
71656	157.199463	192.168.3.12	23.211.195.36	HTTP	1437	GET /places/airports/search?string=New HTTP/1.1
71846	158.036095	192.168.3.12	75.126.75.221	HTTP	836	GET /campaign/rtb/adx/cmradddthis.php?cs_uid=5774c46e1efb7d26 HTTP/1.1
72604	160.991604	192.168.3.12	104.122.76.94	HTTP	980	GET /analyze/utm.html HTTP/1.1
73171	163.868735	192.168.3.12	23.211.195.36	HTTP	1437	GET /places/airports/search?string=Mos HTTP/1.1
73270	164.153726	192.168.3.12	23.211.195.36	HTTP	1438	GET /places/airports/search?string=Mosco HTTP/1.1
73293	164.293655	192.168.3.12	23.211.195.36	HTTP	1439	GET /places/airports/search?string=Mosco HTTP/1.1
73931	168.921291	192.168.3.12	23.211.195.36	HTTP	1467	GET /flights/results/airjson?from=JFK&to=DME&trip_type=OneWay&adults=1&childs=0&infants=0&ver=V2&type=json&class=Economy&airline=&carrier=&search.v HTTP/1.1
74235	170.710862	192.168.3.12	192.200.175.27	HTTP	491	GET /mini-spy-cameras/ HTTP/1.1
74477	171.377720	192.168.3.12	23.211.195.36	HTTP	1514	GET /flights/results/airjson?from=JFK&to=DME&trip_type=OneWay&adults=1&childs=0&infants=0&ver=V2&type=json&class=Economy&airline=&carrier=&search.v HTTP/1.1
74587	171.613061	192.168.3.12	192.200.175.27	HTTP	474	GET /template/menu.css HTTP/1.1
74676	171.820782	192.168.3.12	192.200.175.27	HTTP	485	GET /template/Styles/sgcustom.css HTTP/1.1
74677	171.820935	192.168.3.12	192.200.175.27	HTTP	485	[TCP Fast Retransmission] GET /template/Styles/sgcustom.css HTTP/1.1
74678	171.823005	192.168.3.12	192.200.175.27	HTTP	485	[TCP Fast Retransmission] GET /template/Styles/sgcustom.css HTTP/1.1

Frame 74477: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0

Ethernet II, Src: Intel(R) Ethernet Adapter (82:55:82:55:82:55), Dst: 23.211.195.36

Internet Protocol Version 4, Src: 192.168.3.12, Dst: 23.211.195.36

Transmission Control Protocol, Src Port: 49325, Dst Port: 80, Seq: 13845, Ack: 59986, Len: 1402

Hypertext Transfer Protocol

GET /flights/results/airjson?from=JFK&to=DME&trip\_type=OneWay&adults=1&childs=0&infants=0&ver=V2&type=json&class=Economy&airline=&carrier=&search.v HTTP/1.1

Host: www.cleartrip.com\r\n

User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:48.0) Gecko/20100101 Firefox/48.0\r\n

Accept: \*/\*\r\n

Accept-Language: en-US,en;q=0.5\r\n

Accept-Encoding: gzip, deflate\r\n

X-Requested-With: XMLHttpRequest\r\n

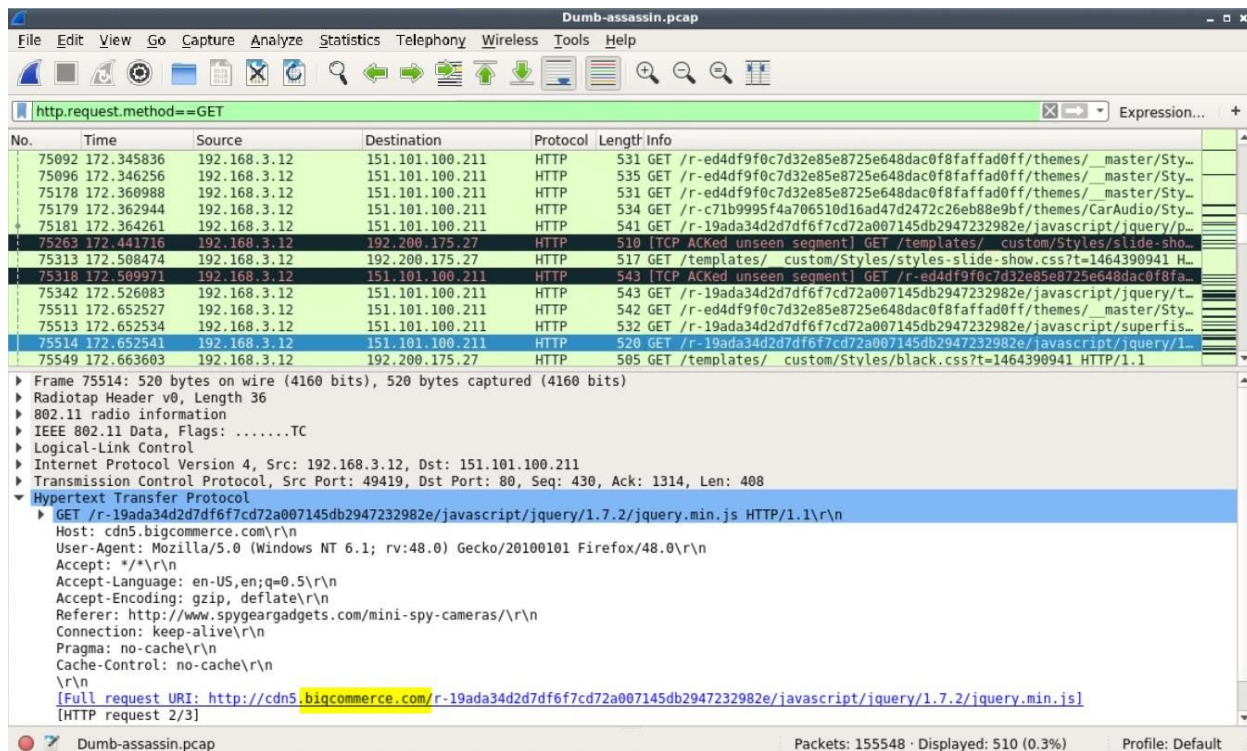
Referer: http://www.cleartrip.com/\r\n

[truncated]Cookie: origin=mum; mob=0; Apache=4050a5fc.5375924e85ddb; ak\_bmsc=47584E1EEF38531C863B9C6D25DAEF8717D3874A1C3B0000EF6C8357BEF90304-plv3\r\n

Full request URI: http://www.cleartrip.com/flights/results/airjson?from=JFK&to=DME&trip\_type=OneWay&adults=1&childs=0&infants=0&ver=V2&type=json&class=Economy&airline=&carrier=&search.v

Packets: 155548 · Displayed: 510 (0.3%) Profile: Default

## Airlines booking one-way flight



The image shows a Wireshark packet capture of a flight booking process. The filter is set to `http.request.method==GET`. The packet list shows several HTTP GET requests to various resources. The selected packet (75514) is a GET request for a jQuery file from cdn5.bigcommerce.com. The packet details pane shows the full request URI and the HTTP request structure.

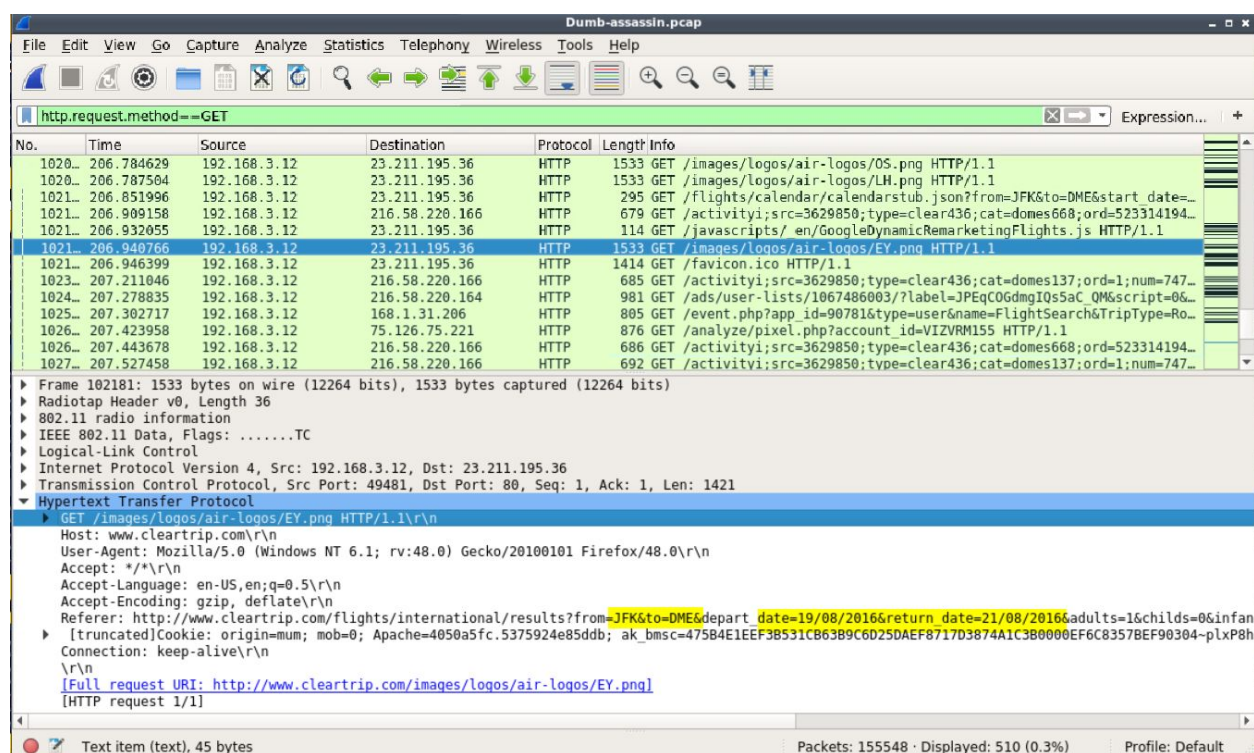
No.	Time	Source	Destination	Protocol	Length	Info
75092	172.345836	192.168.3.12	151.101.100.211	HTTP	531	GET /r-ed4df9f0c7d32e85e8725e648dac0f8affad0ff/themes/_master/Sty...
75096	172.346256	192.168.3.12	151.101.100.211	HTTP	535	GET /r-ed4df9f0c7d32e85e8725e648dac0f8affad0ff/themes/_master/Sty...
75178	172.360988	192.168.3.12	151.101.100.211	HTTP	531	GET /r-ed4df9f0c7d32e85e8725e648dac0f8affad0ff/themes/_master/Sty...
75179	172.362944	192.168.3.12	151.101.100.211	HTTP	534	GET /r-c71b9995f4a706510d16ad47d2472c26eb88e9bf/themes/CarAudio/Sty...
75181	172.364261	192.168.3.12	151.101.100.211	HTTP	541	GET /r-19ada34d2d7df6f7cd72a007145db2947232982e/javascript/jquery/p...
75263	172.441716	192.168.3.12	192.200.175.27	HTTP	510	[TCP ACKed unseen segment] GET /templates/_custom/Styles/slide-sho...
75313	172.508474	192.168.3.12	192.200.175.27	HTTP	517	GET /templates/_custom/Styles/styles-slide-show.css?t=1464390941 H...
75318	172.509971	192.168.3.12	151.101.100.211	HTTP	543	[TCP ACKed unseen segment] GET /r-ed4df9f0c7d32e85e8725e648dac0f8fa...
75342	172.526083	192.168.3.12	151.101.100.211	HTTP	543	GET /r-19ada34d2d7df6f7cd72a007145db2947232982e/javascript/jquery/t...
75511	172.652527	192.168.3.12	151.101.100.211	HTTP	542	GET /r-ed4df9f0c7d32e85e8725e648dac0f8affad0ff/themes/_master/Sty...
75513	172.652534	192.168.3.12	151.101.100.211	HTTP	532	GET /r-19ada34d2d7df6f7cd72a007145db2947232982e/javascript/superfis...
75514	172.652541	192.168.3.12	151.101.100.211	HTTP	520	GET /r-19ada34d2d7df6f7cd72a007145db2947232982e/javascript/jquery/1...
75549	172.663603	192.168.3.12	192.200.175.27	HTTP	505	GET /templates/_custom/Styles/black.css?t=1464390941 HTTP/1.1

Frame 75514: 520 bytes on wire (4160 bits), 520 bytes captured (4160 bits)

- Radiotap Header v0, Length 36
- 802.11 radio information
- IEEE 802.11 Data, Flags: .....TC
- Logical-Link Control
- Internet Protocol Version 4, Src: 192.168.3.12, Dst: 151.101.100.211
- Transmission Control Protocol, Src Port: 49419, Dst Port: 80, Seq: 430, Ack: 1314, Len: 408
- Hypertext Transfer Protocol
  - GET /r-19ada34d2d7df6f7cd72a007145db2947232982e/javascript/jquery/1.7.2/jquery.min.js HTTP/1.1\r\n
  - Host: cdn5.bigcommerce.com\r\n
  - User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:48.0) Gecko/20100101 Firefox/48.0\r\n
  - Accept: \*/\*\r\n
  - Accept-Language: en-US,en;q=0.5\r\n
  - Accept-Encoding: gzip, deflate\r\n
  - Referer: http://www.spygeargadgets.com/mini-spy-cameras/\r\n
  - Connection: keep-alive\r\n
  - Pragma: no-cache\r\n
  - Cache-Control: no-cache\r\n
  - \r\n
  - [Full request URI: <http://cdn5.bigcommerce.com/r-19ada34d2d7df6f7cd72a007145db2947232982e/javascript/jquery/1.7.2/jquery.min.js>]
  - [HTTP request 2/3]

Dumb-assassin.pcap Packets: 155548 · Displayed: 510 (0.3%) Profile: Default

## Airlines booking two-way flight



**Answer:** He browsed for spy tools/gadgets. May be he is planning to use them in his mission. Websites accessed are:

- spygeargadgets.com
- bigcommerce.com

He searched for Air tickets on travel and booking website Clear trip. He searched for

- A one way trip from New York (US) John F. Kennedy (JFK) airport to Moscow (RU) Domodedovo (DME) airport.
- A round trip from New York (US) John F. Kennedy (JFK) airport to Moscow (RU) Domodedovo (DME) airport starting on 19th Aug 2016 and ending on 21st Aug 2016.