From: (b)(6),(b)(7)(C)
Sent: Wednesday, January 05, 2011 6:48 AM
Subject: FW: Building 16

Follow Up Flag: Follow up
Flag Status: Flagged

Suspect as of yet unidentified.

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C)@MIT.EDU]
Sent: Tuesday, January 04, 2011 3:51 PM
To: (b)(6),(b)(7)(C)
Subject: FW: Building 16

(b)(6),(b)(7)(C) here are the screenshots from the camera setup on the laptop at MIT. Looks like he added a drive, but it is still on the network.

(b)(6),(b)(7)(C)

We did not get the call until he left the room.

From: (b)(6),(b)(7)(C)
Sent: Tuesday, January 04, 2011 3:48 PM
To: (b)(6),(b)(7)(C)
Cc: (b)(6),(b)(7)(C)
Subject: Building 16

Here are screenshots from 3:26pm

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)
Information Services & Technology, MIT
(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)mit.edu
(b)(6),(b)(7)(C)

Begin forwarded message:

From: (b)(6),(b)(7)(C)mit.edu>
Date: January 4, 2011 3:46:18 PM EST
To: (b)(6),(b)(7)(C)mit.edu>

(b)(6),(b)(7)(C) (CID)

From: Heymann, Stephen (USAMA) [(b)(6),(b)(7)(C) @usdoj.gov]
Sent: Friday, February 25, 2011 11:31 AM
To: (b)(6),(b)(7)(C) CID)
Subject: RE: Secret Service - Background Information for (b)(6),(b)(7)(C

Does he also have expertise in Linux?

From: (b)(6),(b)(7)(C) CID) [mailto:(b)(6),(b)(7 @usss.dhs.gov]
Sent: Friday, February 25, 2011 11:27 AM
To: Heymann, Stephen (USAMA)
Cc: (b)(6),(b) cert.org
Subject: Secret Service - Background Information for (b)(6),(b)(7)(

Stephen:

Please find the requested background information for (b)(6),(b)(7)(C) has handled Grand Jury information in other cases in other districts.

(b)(6),(b)(7)(C) Member of the Technical Staff, CERT

(b)(6),(is (b)(6),(b)(7)(C) working for CERT's Digital Intelligence and Investigation Directorate (DIID). With over five years experience in the field of Digital Forensics, (b)(6 has conducted forensic investigations in civil and criminal litigation in both the public and private sectors. As a member of the CERT Digital Intelligence and Investigation Directorate (DIID) (b)(6) assists CERT's law enforcement partners in a wide range of digital forensic investigations.

(b)(6),(b holds a number of industry certifications including the Certified Computer Examiner (CCE), EnCase Certified Examiner (EnCE), GIAC Certified Forensic Analyst (GCFA) (b)(6) is also a member of the International Society of Forensic Computer Examiners and the Association of Certified Fraud Examiners (b)(6) obtained a Bachelor of Science degree from Utica College of Syracuse University in Economic Crime Investigation with a concentration in Computer Security.

(b)(6),(b)(7)(C)
Special Agent
U.S. Secret Service
(b)(6),(b)(7)(C) Desk)
Mobile)
412-268-5226 (Fax)

(b)(6),(b)(7)(C) (CID)

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) @usdoj.gov]
Sent: Friday, February 25, 2011 12:16 PM
To: (b)(6),(b)(7)(C) (CID)
Subject: RE: Secret Service - Background Information for (b)(6),(b)(7)(C)

Does he also have expertise in decryption and getting past password protection?

From: (b)(6),(b)(7)(C) CID) [mailto:(b)(6),(b)(7)(@usss.dhs.gov]
Sent: Friday, February 25, 2011 11:34 AM
To: Heymann, Stephen (USAMA)
Subject: Re: Secret Service - Background Information for b(6) b7C

He has expertise in Windows, Linux, BSD, VMFS (VMware's file system), and OS X.

(b)(6),(b)(7)(C)
Special Agent
U.S. Secret Service
(b)(6),(b)(7)(C) (Desk)
(Mobile)
412-288-5226 (Fax)

From: Heymann, Stephen (USAMA (b)(6),(b)(7)(C) usdoj.gov>
To: (b)(6),(b)(7)(C) (CID)
Sent: Fri Feb 25 11:30:47 2011
Subject: RE: Secret Service - Background Information fo (b)(6),(b)(7)(C

Does he also have expertise in Linux?

From: (b)(6),(b)(7)((CID) [mailto:(b)(6),(b)(7) usss.dhs.gov]
Sent: Friday, February 25, 2011 11:27 AM
To: Heymann, Stephen (USAMA)
Cc: (b)(6),(b)(ert.org
Subject: Secret Service - Background Information fo (b)(6),(b)(7)(

Stephen:

Please find the requested background information for (b)(6),(b)(7)(C) has handled Grand Jury information in other cases in other districts.

(b)(6),(b)(7)(C Member of the Technical Staff, CERT

(b)(6), (b)(6),(b)(7)(C) working for CERT's Digital Intelligence and Investigation Directorate (DIID). With over five years experience in the field of Digital Forensics, (b)(6) has conducted forensic investigations in civil and criminal litigation in both the (b)(6),(b)(7)(C) As a member of the CERT Digital Intelligence and Investigation Directorate (DIID), (b)(6) assists CERT's law enforcement partners in a wide range of digital forensic investigations.

(b)(6) holds a number of industry certifications including the Certified Computer Examiner (CCE), EnCase Certified Examiner (EnCE), GIAC Certified Forensic Analyst (GCFA) (b)(6) is also a member of the International Society of Forensic Computer Examiners and the Association of Certified Fraud Examiners (b)(6) obtained a Bachelor of Science degree from Utica College of Syracuse University in Economic Crime Investigation with a concentration in Computer Security.

(b)(6),(b)(7)(C)

UNITED STATES GOVERNMENT

Memorandum of interview

DATE AND TIME: September 13th, 2012

U.S. Secret Service

LOCATION: 301 East Liberty Street, Ann Arbor, MI

Case # 102-775-60071-S

SUBJECT INTERVIEWED: (b)(6),(b)(7)(C)

IN ATTENDANCE:
SA (b)(6),(b)(7)(C) (BOS)
Detective (b)(6),(b)(7)(C) Cambridge Police
AUSA Stephen Heymann
AUSA (b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)

On September 13th, 2012 (b)(6),(b)(7)(C) was interviewed at the JSTOR office at 301 East Liberty Street, Ann Arbor, MI, in reference to the Boston Field Office case number 102-775-60071-S. The interview was conducted by Agent (b)(6),(b)(7)(C) and Cambridge Police Detective (b)(6),(b)(7)(C) Also in attendance were AUSA Stephen Heymann, AUSA (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) The following is a summary of his statements:

(b)(6),(b)(7)(C) stated that he was (b)(6),(b)(7)(C) He stated that JSTOR is the biggest part of Ithanka and that more than 10,000 institutions were supported. (b)(6),(b) stated that he was involved with tech support, web site support and access, and abuse monitoring and prevention. (b)(6),(b) stated that he was involved with the load balancing of three data centers in Princeton New Jersey, Manchester United Kingdom and Ann Arbor Michigan.

(b)(6),(b) stated that JSTOR used Literatum from Atypon and that Literatum has abuse monitoring tools. (b)(6),(b)(stated that the terms and conditions for using JSTOR prohibit mass downloading. (b)(6),(b)(7 stated that if a user has a registered account he must log in and acknowledge the terms and conditions. If a user does not have a registered account he must acknowledge the terms and conditions each time he engages JSTOR. JSTOR had previously implemented Literatum abuse tools to block when 5,000 sessions are created from the same IP in a 60 minute period. (b)(6),(b) stated that JSTOR has a web site with information on how researchers can download data sets for projects. (b)(6),(b) stated that a session was defined by machine ID and a cookie and a session was designed to time out after 20 to 30 minutes of inactivity. (b)(6), (b)(7)(C) stated that JSTOR had a download limit of 300 articles.

(b)(6),(b) (7)(C) stated that on 09/25/10 (b)(6),(b)(7)(C) told him that he received an alert from the Manchester server with activity that looked like a PDF scraper. (b)(6),(b) stated that on 09/26/12 (b)(6),(b) told him that he noticed the PDF scrapper again on IP address (b)(6),(b)(7)(C). (b)(6), (b)(7)(stated that JSTOR blocked access to the Class C IP range of the IP address.

(b)(6),(b) stated that on 10/09/10 at around 1745 he had noticed that the PDF scrapper had come back and that by 1814 half of the servers in Manchester had failed under the strain of the downloads and had to be restarted.

(b)(6),(b) stated that JSTOR implemented Literatum abuse tools to block when 5,000 sessions are created from the same IP address in a 60 minute period.