

①

CAN over 655
IP 187.

5:42 pm 13-Sept-12

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

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

Computer Scientist - Technology

Has learned to do Data Analysis

Started doing Analysis of Logs

End of 2010 beginning 2011

He found the download

Can parse by IP & Date

Can get down to milliseconds -

IP Address

User Agent: Software program the user

is using to harvest the data

He can tell how many PDF's

User Agents to download

IP Address

Duration of Session or User Visit

User Agent = Web Browser, Scripting Language

Rather than a browser - "CURL"

(guess) → Suspect perl was the language

Cur! / 7.19.7... user

6:30 pm

PREPARED BY	MIT
DATE	

	PAGE
	NO.

2nd

China

→

2nd

1:48 pm

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

Oct 9 J&J

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

SLASH.005 Article
Amazon EC2

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

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

Australia

Still unknown

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

ARP Table - Contains IP
IP Addresses & Mac Addresses
was giving

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

Jan 3rd
MIT

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

gets access to

PREPARED BY: [redacted]
DATE: 1/14/13

MEET Interview
(b)(6), (b)(7)(C)

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

Arvo Suster Case
Present MEET Eq. (b)(6), (b)(7)(C)

Religious
Library
(b)(6), (b)(7)(C)

MEET's relationship w/ JStar
What is the value of
JStar subscription?

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

1987 started JStar
Subscription
\$435,000. Paid to date
\$50,000 per year fee
Eight collections produced
#9 still to purchase
Archive Capital Fee
→ 1st Fee
Top Tier Membership for MEET

PREPARED BY
DATE

PAGE NO.

PROJECT ACTG. NOTES

PROJECT PLANNING NOTES

ADD Table

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

Jan 3rd

mapped the IP address to the switch

NEED COPY OF

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

NOTES After (b)(6), (b)(7)(C) - mapped IP address.

Can you tell what customer was for a secure shell to another place?

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

- All SSH Traffic

is bound to Netbox
19. Different IPs
Port SSH into Netbox
Search
Do DHEC Cuneless

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

Copy of the file

Copy File 2
Same as next into the netbook.

Friday WED

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

2nd (b)(6), (b)(7)(C)

In kind Copy file

2, 4, 09

Linux

Linux. edu

Linux Dual to Server

pg 2

(b)(8),(b)(7)(C)

was there
was there

"Director followed" No to installing
camera -

(b)(8),(b)(7)(C)

was there?

(b)(8),(b)(7)(C)

(b)(8),(b)(7)(C)

Saw cable going into Netbank
with an external storage device attached
under a box.

The Netbank was never tested - mem-

Packet Sniffing = Doesn't remember

Does not remember telling (b)(8),(b)(7)(C)
to install camera nor does he normally
tell (b)(8),(b)(7)(C) to do camera installs.

Encl. 955 mg

page 2, 12/10/12

How does the network pick up

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

?

Can MIT tell if (b)(6),(b)(7)(C) used to DHCP?

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

= There were with occasions when AS did not use DHCP to obtain IP addresses.

SH can you tell if DHCP gave an IP?

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

6.240
7.240

No DHCP records in Nov 2010

SH: 11/22 -> 12/26

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

was used.

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

Has some Sept ²⁰¹⁰ logs
Earliest dates of logs

SH Instructs which days we have DHCP logs?
Send to (b)(6),(b)(7)(C) for distribution.

Linux can set up

SH when you look for IP ending .240

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

find it by using ARP TABLE
which is a map for MAC addresses & IP'S

MAC

on system.

Address Resolution Protocol = ARP

ARP Table is what

(b)(8), (b)(7)(C)

 used to find the IP Address using MAC & Matched the MAC Address.

MAC Addresses are used in local networks
IP's used on Internet.

page 1

Jan 3, 2013
9:30am

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

Stephen Heywood
ME

SH Begins by stating of case / investigation
to (b)(6), (b)(7)(C)

SH tells (b)(6), (b)(7)(C) that he is to
be witness on 1-25-13 for mistrial.
And Trial for 4-1-13 - middle to
end of week 1 of Trial

MR → Tell (b)(6), (b)(7)(C) that he don't do anything wrong

ME → Tell him to rephrase the question!

ME → Point your fear at jury for Trial &
and Judge for hearing.

(b)(6), (b)(7)(C) = discuss social traffic between
him & others for a few minutes -

→ (b)(6), (b)(7)(C) Answers 9:40 am

(b)(6), (b)(7)(C) - Asked (b)(6), (b)(7)(C) if he has testified &
explains the testimony function

(b)(6), (b)(7)(C) - starts

#1

MIT Interviews JAN 3, 2013

1:47pm

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

Steve Heyman

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

SH

SH = Gives (b)(6),(b)(7)(C) starts - f
Case - Trial - Motions - Etc

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

has met

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

SH: what are the intended rules of the
network?

What can be enforced?

What is the practical stuff that happens?

When you go for Guest Logon? Is it rule?

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

→ Yes it is!

SH → Is it a rule that you can enforce?

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

→ The 14 Day Rule was enforced in

2005-2011 - A counter was in place to
log

SH = what is (b)(6),(b)(7)(C) Role -

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

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

of IT Security Support

= They responded to incidents i.e. an
event occurred that was reported to them