

Date: Mon, 21 Oct 2019 4:01:12 PM (UTC)
Sent: Mon, 21 Oct 2019 4:01:14 PM (UTC)
Subject: RE: Keychain cracking --- UNCLASSIFIED
From: [REDACTED]
To: [REDACTED]
CC: [REDACTED]

Classification: UNCLASSIFIED

We tried to do an EC way back when, but the case classification did not allow for us to do it. The UCFN is 31E-NY-3027571 (Epstein)

[REDACTED]
Senior Forensic Examiner
[REDACTED] Office)
[REDACTED] Cell)
[REDACTED] (Fax)

From: [REDACTED]
Sent: Monday, October 21, 2019 11:32 AM
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: Keychain cracking --- UNCLASSIFIED

Classification: UNCLASSIFIED

Hey there,
DID we have an EC/Lead for this? Or a UCFN for tracking purposes?

Trying to document this for our records (and yours potentially)

Let me know.

Thanks

From: [REDACTED]
Sent: Monday, October 21, 2019 11:20 AM
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: Keychain cracking --- UNCLASSIFIED

Classification: UNCLASSIFIED

=====

I've said it before, and I'll say it again. THERE IS NOBODY BETTER THAN YOU GUYS!!!! Thanks. The password you provided unlocked the drive. I owe you a beer.

[REDACTED]
Senior Forensic Examiner

[REDACTED]

From: [REDACTED]
Sent: Monday, October 21, 2019 11:14 AM
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: Keychain cracking --- UNCLASSIFIED

Classification: UNCLASSIFIED

=====

Good morning [REDACTED]

STXU has recovered a password "asdfasdfasdf" (no quotes) for item NYC024364.

Once your forensic analysis is complete, a brief summary (a few sentences) as to the value of STXU's efforts/password provided is appreciated when convenient. This helps STXU focus our expertise and streamline decryption efforts in support of future investigations.

STXU will remove all copies of this data and considers this request complete.

Please contact STXU for further dissemination of these results outside of the FBI. If you have any further questions, please contact EE [REDACTED] at [REDACTED]

If everything looks good and you have no further questions, please "remove HQU-VAP permissions in the CAT tool".

[REDACTED]
IT Specialist / Senior Forensic Examiner

Secure Technologies Exploitation Unit (STXU)
Operational Technology Division (OTD) - Miami

[REDACTED]

From: [REDACTED]
Sent: Thursday, October 17, 2019 12:16 PM
To: [REDACTED]
Cc: [REDACTED]

SUBJECT TO PROTECTIVE ORDER PARAGRAPHS 7, 8, 9, 10, 15, and 17

Subject: RE: Keychain cracking --- UNCLASSIFIED

Classification: UNCLASSIFIED

Yes. I'll make sure you have permissions. The image can be found at
//NYCART-FS/Cases01/ny-3027571_219047/Evidence/NYC024364 It is a 1 TB E01.

[REDACTED]
Senior Forensic Examiner

From: [REDACTED]
Sent: Thursday, October 17, 2019 11:58 AM
To: [REDACTED]
Cc: [REDACTED]

Subject: RE: Keychain cracking --- UNCLASSIFIED

Classification: UNCLASSIFIED

Is the image on OPWAN so I can take a look at it?

Thank you,

[REDACTED]

From: [REDACTED]
Sent: Thursday, October 17, 2019 11:56 AM
To: [REDACTED]
Cc: [REDACTED]

Subject: RE: Keychain cracking --- UNCLASSIFIED

Classification: UNCLASSIFIED

It isn't a T2 system, but I was having many difficulties acquiring the drive with Macquisition, so I had to remove the drive and use a TX1. This is not the latest generation of MacBook, I believe it is the generation right after they removed the CD drive, so it is recent, but not brand new. It is very possible that this was somebody else's machine, but without being able to browse the usernames, I can't be 100% certain.

[REDACTED]
Senior Forensic Examiner

(212)384-4838 (Office)
(917)855-6666 (Cell)
(212)384-1334 (Fax)

From: [REDACTED] (OTD) (FBI)
Sent: Thursday, October 17, 2019 9:40 AM
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: Keychain cracking --- UNCLASSIFIED

Classification: UNCLASSIFIED

Good morning [REDACTED] Is this a T2 system as well? Also, do you have any indication of who the user of the laptop may have been? As I recall, there was at least one system that I looked at when I was working on the original request that was used by someone other than him. Please let me know.

Thank you!

From: [REDACTED] (NY) (FBI)
Sent: Wednesday, October 16, 2019 12:55 PM
To: [REDACTED]
Subject: RE: Keychain cracking --- UNCLASSIFIED

Classification: UNCLASSIFIED

Hey [REDACTED]
I have another MacBook Pro that is locked for the same case. The password hint is "stroke4". The passwords below did not work. Any help is appreciated. Thanks.

[REDACTED]
Senior Forensic Examiner
[REDACTED]

From: [REDACTED]
Sent: Thursday, September 05, 2019 10:56 AM
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: Keychain cracking --- UNCLASSIFIED

3503-011
Page 4 of 8

SUBJECT TO PROTECTIVE ORDER PARAGRAPHS 7, 8, 9, 10, 15, and 17

EFTA_00001901

EFTA00157086

Classification: UNCLASSIFIED

I'm glad we could be of assistance. Please let us know if you need anything else and don't forget to send us an update once your forensic analysis is complete. A brief summary (a few sentences) as to the value of STXU's efforts/password provided is appreciated when convenient as this helps STXU focus our expertise and streamline decryption efforts in support of future investigations.

Thank you,

From: [REDACTED] (NY) (FBI)
Sent: Thursday, September 05, 2019 10:50 AM
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: Keychain cracking --- UNCLASSIFIED

Classification: UNCLASSIFIED

[REDACTED]
You guys are great. The password "irving" worked. I am now in the machine and imaging it. Thanks for all your help. I obviously could not have done it without you.

[REDACTED]
Senior Forensic Examiner
[REDACTED]

From: [REDACTED]
Sent: Thursday, September 05, 2019 9:47 AM
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: Keychain cracking --- UNCLASSIFIED

Classification: UNCLASSIFIED

Oh yes, NYC024353 was the one with the user account JEE and I had already obtained the user password as part of your previous request which was 'irving' (no quotes). In his keychain he had the following passwords which you can try:

irvingirving
neptunemermaid [this one was used extensively]
asdfasdf [this was used for a Gmail account]
yes8"tin [this was the password for his multiple AirPort routers]

Please let me know your results once you try them so I can update our internal system accordingly regarding your request.

3503-011
Page 5 of 8

SUBJECT TO PROTECTIVE ORDER PARAGRAPHS 7, 8, 9, 10, 15, and 17

EFTA_00001902

EFTA00157087

Thank you!

[REDACTED]

From: [REDACTED]
Sent: Thursday, September 05, 2019 8:53 AM
To: [REDACTED]
Subject: RE: Keychain cracking --- UNCLASSIFIED

Classification: UNCLASSIFIED

The machines in question are Macs running APFS, and their images are aff4 files. I have them here in Blacklight, but I can't confirm which one because the Case Agents are using my one Blacklight machine to review. The images are NYC024353 and NYC024329. One of them has a user account of JEE or a similar username which is obviously the subject. If you have a list of possible passwords, could you forward that for me to try on the T2 iMac?

[REDACTED]
Senior Forensic Examiner
[REDACTED]

From: [REDACTED]
Sent: Thursday, September 05, 2019 8:43 AM
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: Keychain cracking --- UNCLASSIFIED

Classification: UNCLASSIFIED

Good morning [REDACTED] I can certainly try. When I worked on your request I was able to recover several passwords for him from other systems (and their keychains) that were provided so I may already have it. Which ones did you want me to check?

Let me know and I'll take a look at it.

[REDACTED]
IT Specialist / Senior Forensic Examiner

Secure Technologies Exploitation Unit (STXU)
Operational Technology Division (OTD) - Miami
[REDACTED]

From: [REDACTED]

Sent: Wednesday, September 04, 2019 3:35 PM
To: [REDACTED]
Subject: Keychain cracking --- UNCLASSIFIED

=====
Classification: UNCLASSIFIED
=====

[REDACTED]

You seem to be the Mac guy for your unit. Quick question. If I give you an un-encrypted image of a Mac either in APFS or HFS+, would you be able to recover the password for the user account? I have multiple images of macs from Epstein, and they all have the same password hint. Figuring he just used the data migration tool and rolled everything along. Hope it can give us a password for a T2 iMac we can't get an image of.

[REDACTED]
NYOCART Coordinator
Senior Forensic Examiner
[REDACTED]

=====
Classification: UNCLASSIFIED
=====

Classification: UNCLASSIFIED

Classification: UNCLASSIFIED

Classification: UNCLASSIFIED

Classification: UNCLASSIFIED

Classification: UNCLASSIFIED

SUBJECT TO PROTECTIVE ORDER PARAGRAPHS 7, 8, 9, 10, 15, and 17