Alexander Cannell

5/2/13

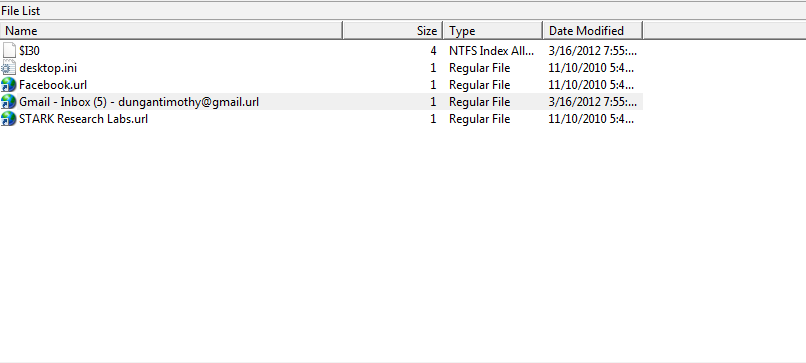
Professor Robertson

TDungan Final:

**Introduction:**

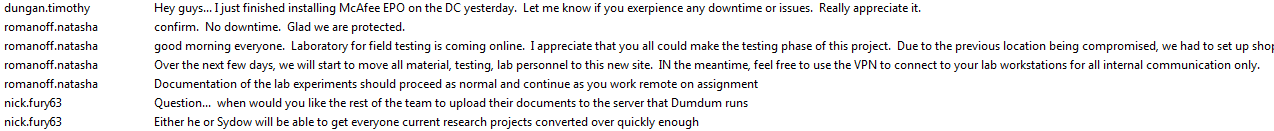
This is the introduction to our Network Forensics Final. We as a class examined Tim Dungan machine for suspicious activity. I used FTK Light, Web Historian, Excel, OSForensics, and SkypeView.

**Examination:**



Looking at Tdungans Favorites I found his Gmail dungantimothy@gmail.com.

Alex Cannell 4/27

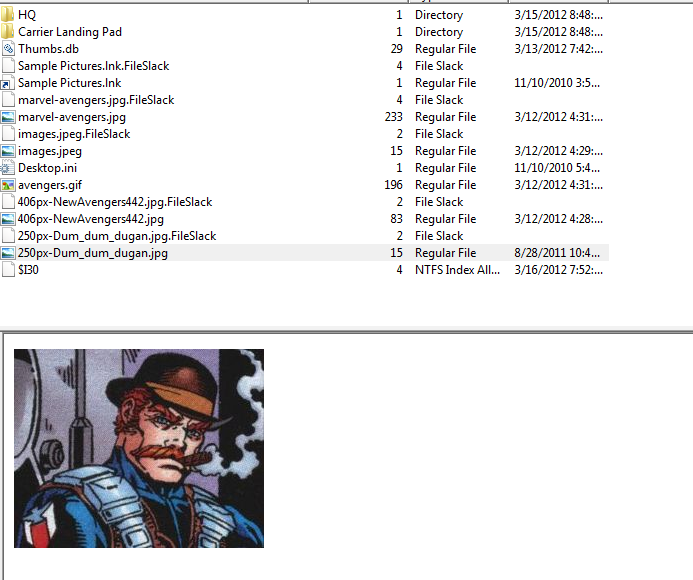


It looks like Tim Duncan(Skype ID = dungan.timothy) installed McAfee on DC(Im assuming DC is a server) on 09/17/2011 at 10:34:32 AMand he was relaying this information to Natasha Romanoff (Skype ID = romanoff.natasha)who promptly responded with a confirmation of no downtime on the DC.

Several Months later on 03/05/2012 at 7:50:17 AM Natasha Romanoff informed everyone, “good morning everyone.  Laboratory for field testing is coming online.  I appreciate that you all could make the testing phase of this project.  Due to the previous location being compromised, we had to set up shop within stark-research-labs.  As our backup laboratory, all future testing will be accomplished here. Over the next few days, we will start to move all material, testing, lab personnel to this new site.  IN the meantime, feel free to use the VPN to connect to your lab workstations for all internal communication only. Documentation of the lab experiments should proceed as normal and continue as you work remote on assignment...”

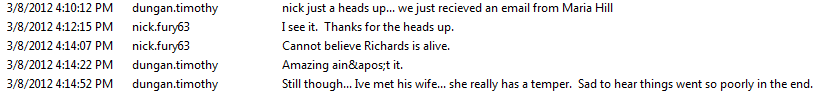
Right after Nick Fury (Skype ID = nick.fury63) asked when they could upload their documentation to the Dumdum server. He continues with his confidence that the reasearch project could be converted over quickly enough.

Alex Cannell 4/27



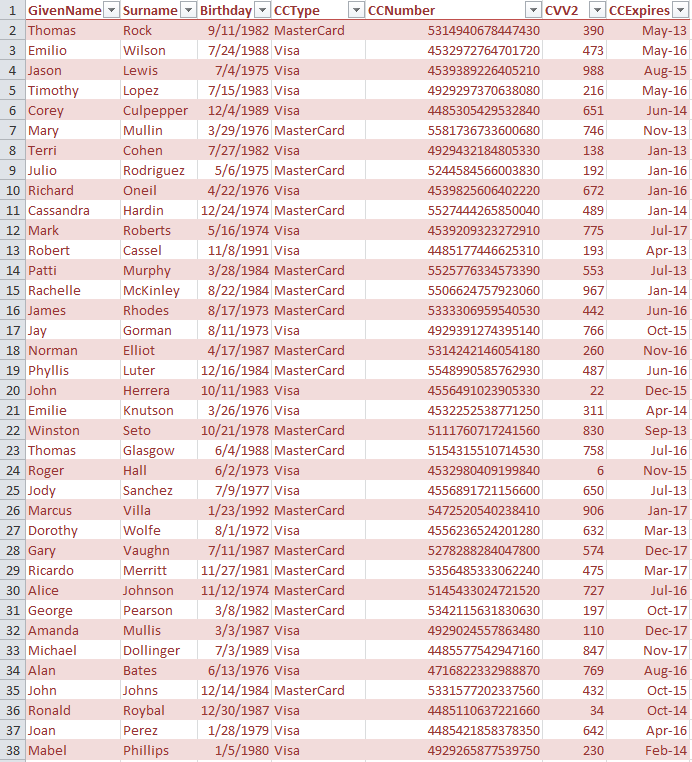
Found out who DumDum is from Nick Fury’s skype, “Right after Nick Fury (Skype ID = nick.fury63) asked when they could upload their documentation to the Dumdum server. He continues with his confidence that the research project could be converted over quickly enough.” It is actually Tim Dungan.

I also found some pictures of HQ and of their Landing Pad in Tim Dungans files. (and a whole lot of pictures of the avengers.

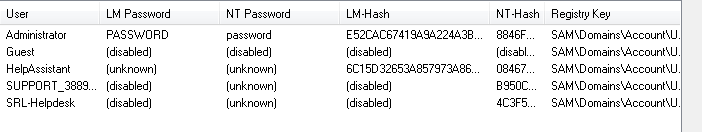
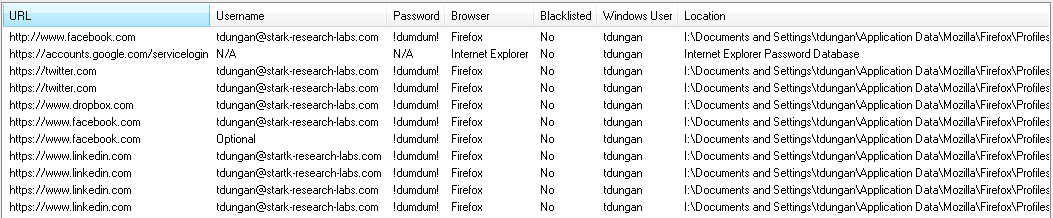
Alex Cannell 4/30

Tim Dungan informed Nick Fury about Maria Hills email.

They continue talking about someone called Richards who is still alive and his wife. Time replied with, “Amazing ain&apos;t it.” dont know what “ain&apos;t” means.  I assume that they are talking about Richard Fisk (antihero) and his wife Vanessa.

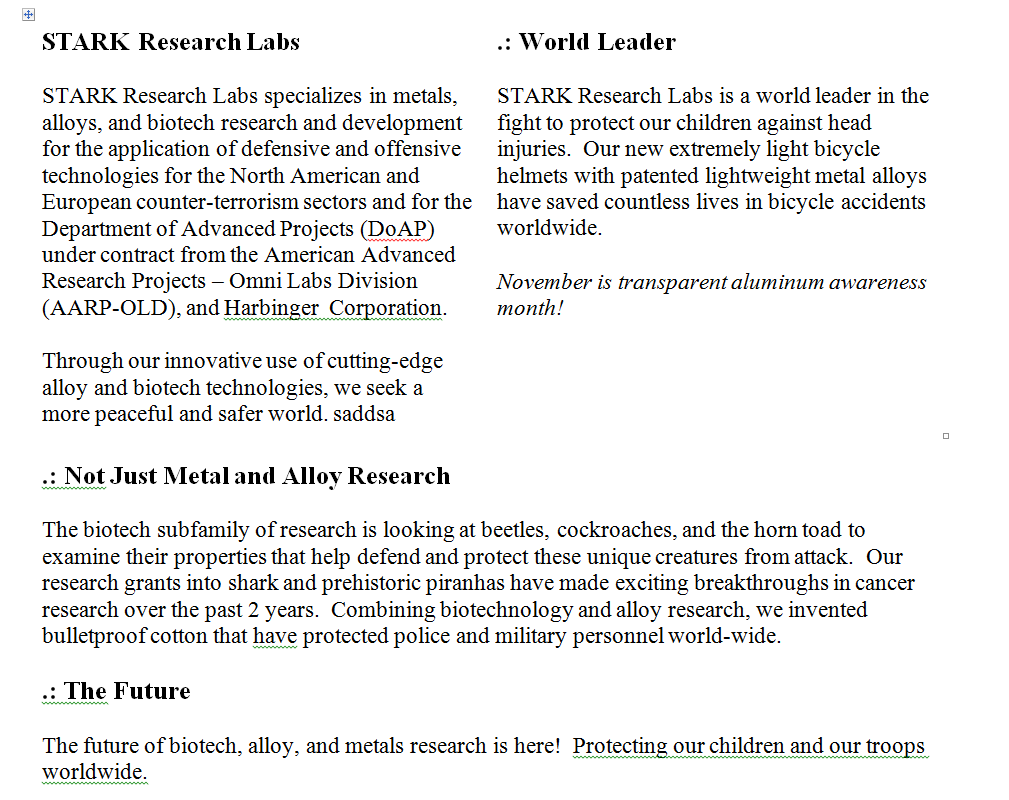
Alex Cannell 4/27

I found 251 Credit card numbers, names, birthdays, Card Types, CVV2 Numbers, and Card Expiration dates. which was modified last on 4/3/2012, in location /tdungan/Documents and Settings/MyDocuments/Backstoped Accounts -RDcosts Alloy Research/.

Alex Cannell 4/30

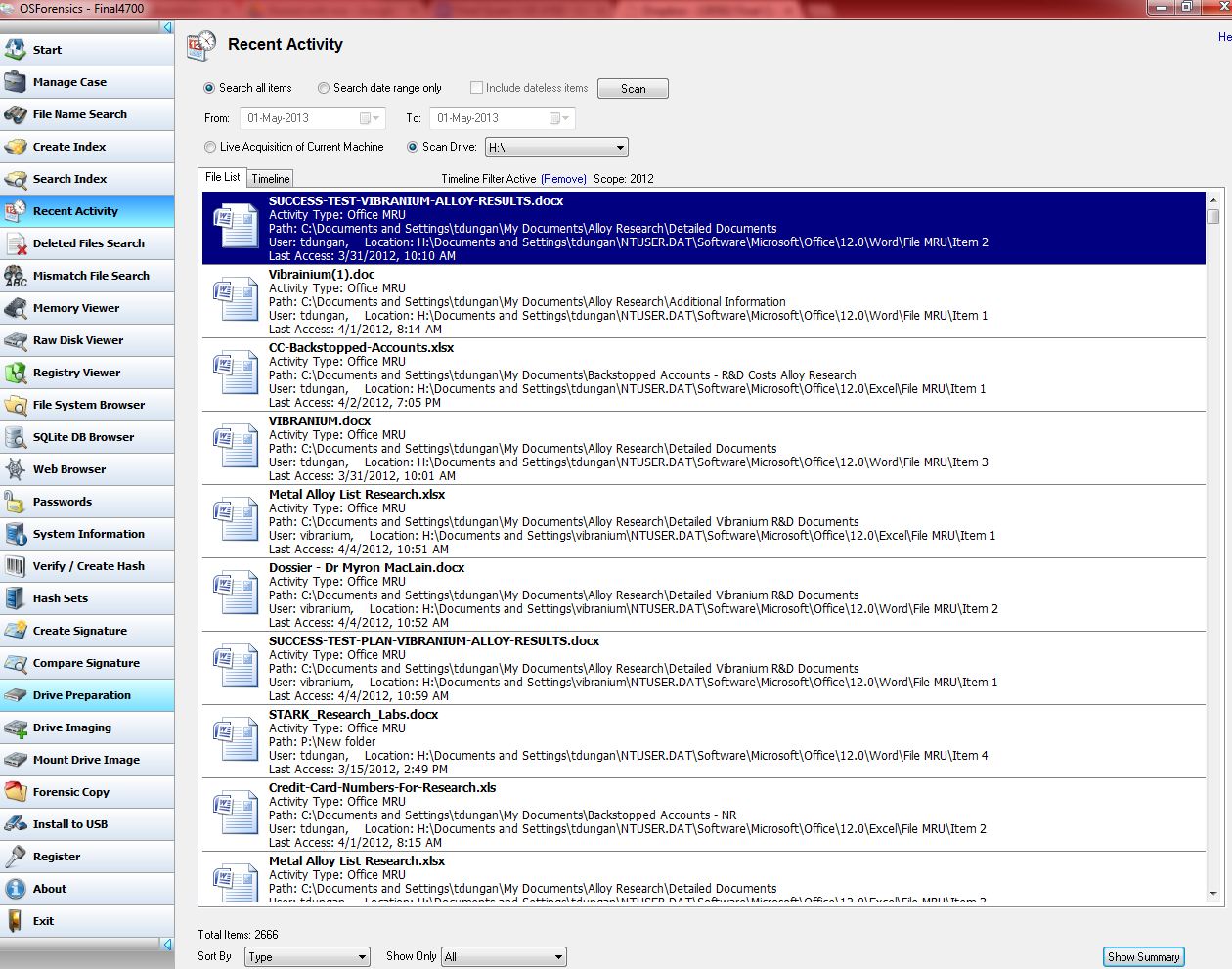
I found his social media passwords, and his administrator password(which is very secure). I used OSforensics to retrieve this information.

Alex Cannell and Ethan Kleinman 5/1



This was the last final that inputed into dropbox, the files name is STARK Research Labs.dox. I found this by going to \Dropbox\.dropbox.cashe.

Alex Cannell and Ethan Kleinman 5/2

Using the software OSforensics I compiled a timeline that includes all recently accessed documents, I also added some of the websites that caught my attention.

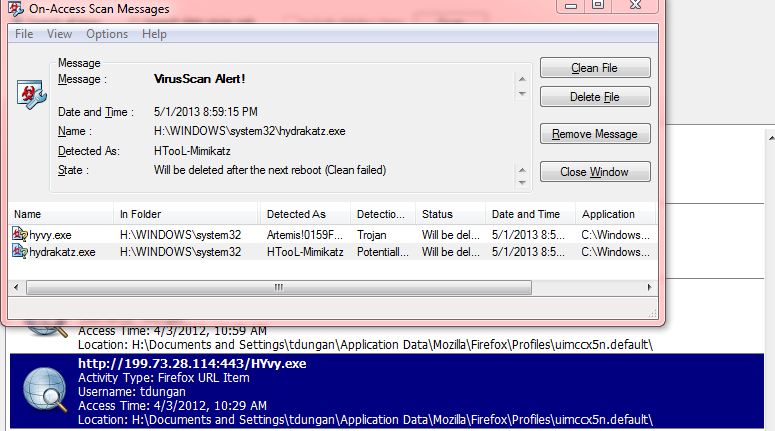
Here is the link to the document timeline ->

<https://docs.google.com/spreadsheet/ccc?key=0AkgCktRI38R4dFpqTlBCZ09OWVZOMTRpb0RpdWoxMmc&usp=sharing>

The document timeline wont export in excel with file names so here it is in text format that includes the filenames -> <https://docs.google.com/file/d/0B0gCktRI38R4Y1N5UmQxU0RjdjQ/edit?usp=sharing>

The two timelines correspond directly

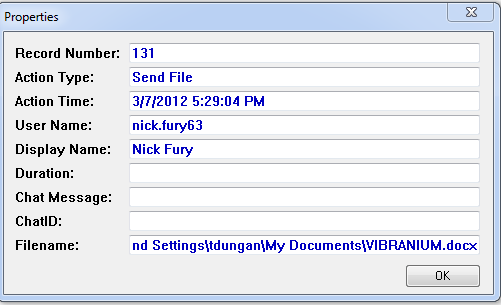
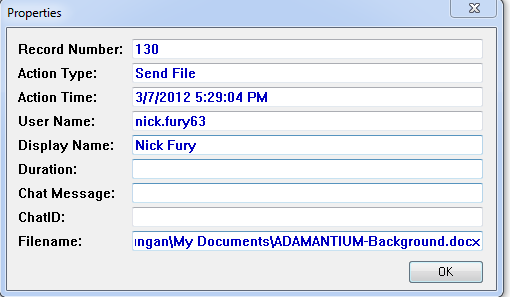
I also found FireFox history with the file “HYvy.exe” being downloaded from “<http://199.73.28.114:443/HYvy.exe>”

This file was downloaded to the system32 folder and is detected as a Trojan 

Here is a link to the entire timeline in csv format ->

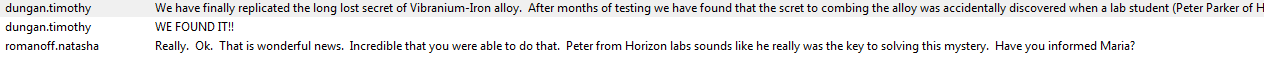
<https://docs.google.com/file/d/0B0gCktRI38R4WE51djhiel8zUmM/edit?usp=sharing>

Ethan Kleinman  5/1

https://lh6.googleusercontent.com/frZ9Mve02zIECimIpYx_R-I0O2ytB-ZMrdU5fFg5RP3-i1dhqqQB1OJoOhlRy5S2bSHAoQmPGYK4WiedONy__TCZEHO_CG07mensHdZSb2U8OY6VdGI-Zpo2_g

Looking at the Skype Chat logs,Tim Dungan Sent two documents to Nick Fury through Skype. The Files are ADAMANTIUM\_Background.docx and VIBRANIUM.docx.

Alex Cannell 4/27



On 03/31/2012 at 10:08:05 AM on Skype Tim Duncan informs everyone that they had found the Vibranium-Iron Alloy, which was discovered by Peter Parker at Horizon Labs.

Alex Cannell 4/27

**Conclusion:**

I started examining Tim Dungan’s machine with the examination of the favorites file. I was able to find he had marked Facebook, Stark research lab website, and his gmail. His gmail is dungantimothy@gmail.com. I then examined the skype logs where I found communications between Natasha Romanoff, Nick Fury, and Tim Dungan. It looks like Tim Duncan (Skype ID = dungan.timothy) installed McAfee on DC (I’m assuming DC is a server) on 09/17/2011 at 10:34:32 AM. He was relaying this information to Natasha Romanoff (Skype ID = romanoff.natasha) who promptly responded with a confirmation of no downtime on the DC. Right after Nick Fury (Skype ID = nick.fury63) asked when they could upload their documentation to the Dumdum server. He continues with his confidence that the research project could be converted over quickly enough. I also found who the dumdum server is from Nick Fury’s Skype post. I found 251 credit card numbers, names, birthdays, card types, cvv2 numbers, and card expiration dates. This information is something that Tim doesn’t want to lose, or miss place. I found his social media passwords, and his administrator password (which is very secure). I found that the last thing we found was sent through dropbox was STARKResearchLabs.dox. On skype logs I found evidence that they had found the Vibranium-iron alloy. Ethan and I worked on the timeline together.

**Suggestions:**

From what I found Tim really needs to increase his security. Tim’s passwords are pitiful, I would suggest that he try password strength testers. <http://www.passwordmeter.com/> Tim also should encrypt his sensitive data like the credit card information (I would try truecrypt). <http://www.truecrypt.org/>

SIDE NOTE JOKE:

