Group Members:-

Muhammad Izham Bin Norhamadi, B032020039, S2G1

Ahmad Sha Herizam Bin Tahir. B032020009, S2G1

Affendy Elyas bin Azhari Sharidan, B032020024, S2G1

5.1.2 Task

a. What is the case (nature of case)?

Fraud, scam, drug trafficking, and credit card theft.

b. What evidence supports the case?

Message0004

Subject: Re: New Venture
From: "John Washer" <chkwasher@comcast.net>
Date: Wed, 11 Jul 2007 14:27:15 -0600
To: "Wes Mantooth" <dollarhyde86@comcast.net>, "Mr Smee" <smee.rox@gmail.com>

Message Body

Sweet!

If that turns out to be too risky, a budy of mine showed me how to rig the machines to keep the cards... Then we shoulder surf the pin and get the card when they leave!

He got this from a SPAM chainletter!

I love it!

----- Original Message -----
From: Wes Mantooth
To: Mr Smee
Cc: John Washer
Sent: Thursday, July 12, 2007 5:19 PM
Subject: New Venture

I am thinking we should launch into a new venture...

Take a look at this and tell me what you think. I can get the parts for about $100.

Word

Attachment

-----Attachment2-----
File name = "ATM_THEFTS1.ppt"

Figure 1: Email between John Washer and Wes Mantooth about ATM theft

Figure 2: ppt file identified in both images regarding ATM theft

From: John Washer [mailto:chkwasher@comcast.net]
Sent: Monday, July 23, 2007 12:59 PM
To: txkidd@swbell.net
Cc: Mantooth
Subject: Stuff

Rosco,

I got your name from Wes. He says that you are the GOTO guy for the kinda stuff I am into.

;) DIDN'T YOU WES!

Anywaze... We should get together sometime and I can show you my "goods". I am getting pretty good at my trade.

In the meantime, we will keep our new relationship on the QT via Email.

Let me know if I can help you in any way with your ventures.

John

Figure 3: John got introduced to Rosco by Wes

Message0008	
Subject:	**You will love this....**
From:	"Rasco Badguy" <txkidd@swbell.net>
Date:	Mon, 23 Jul 2007 16:26:10 -0500
To:	"'John Washer'" <chkwasher@comcast.net>
CC:	"'Wes Mantooth'" <dollarhyde86@comcast.net>
Message Body	
This doc says it all guys.....ran across it and my buddy skimmerman used it a few times.....worked like a charm..... R~	
Attachment	
-----Attachment2----- File name = "How To Steal Credit Numbers.doc"	

Figure 4: Rasco share to John and Wes how to steal credit card number.

How To Steal Credit Numbers

Ok this information is about the same as how to steal passwords but its credit cards your stealing this time.

First off aol has a passprogram that not only has to do with passwords but also credit card numbers off of aol billing. So what you do is go to write email and put passprogram@aol in the send box.

Next- in the subject box put in h-kte-429-2391- so aol gets a message that will let you by the pass block. Next go to the first line (where you would write an email) and type your screen name and real-credit card number and the name on the credit card, so the reciever will read it an send it past thinking you are going into your billing account.

Next- in the 2nd line put in a fake persons name like ,joe brown and that fake person would be likely to be in aol billing. If not try a different name. Next in the 3rd line put in nothing , just leave it blank
and that is it in one day aol will send you the credit card number of whoever you wanted. It is even eaiser than stealing passwords.

Figure 5: How To Steal Credit Numbers.doc

1234 5678 1234 1234	232	10/09	M
0012 3330 3330 3030	676	03/10	M
2145 0909 9888 0989	998	02/10	V
1929 000986 12345	4253	11/09	A

Figure 6: SLIST.doc lists some of the stolen credit card information

From: John Washer [mailto:chkwasher@comcast.net]
Sent: Wednesday, June 20, 2007 11:56 AM
To: Mantooth
Subject: Whats up in D town?

Dude!

You been laying a little low these days?

I have been trying to call you almost daily and we can't hook up!

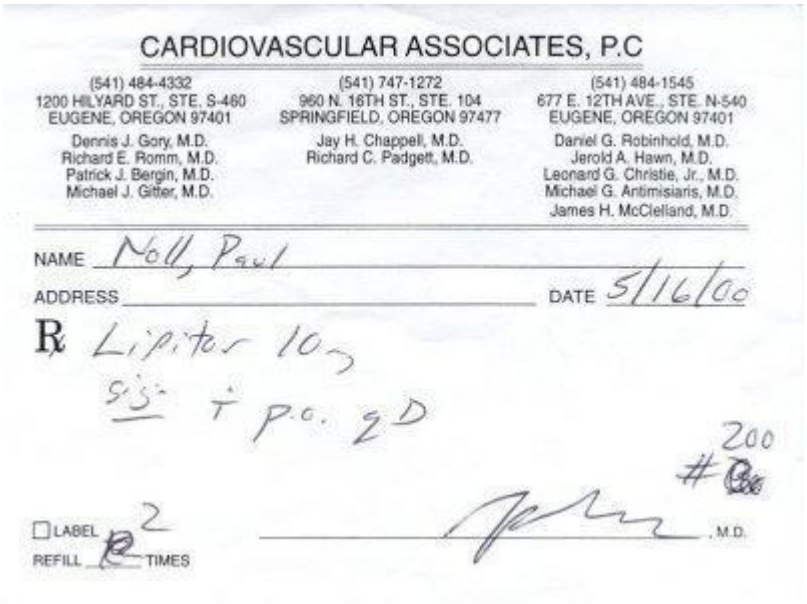
I have the "Special K" your looking for... but it is going to cost you!

Give me a buzz! But hurry... this stuff ain't gonna last!

Attachment

-----Attachment2-----
File name = "doc-prescription.jpg"

Figure 7: Exchange about a drug called “Special K”


CARDIOVASCULAR ASSOCIATES, P.C

(541) 484-4332
1200 HILYARD ST., STE. S-460
EUGENE, OREGON 97401
Dennis J. Gory, M.D.
Richard E. Romm, M.D.
Patrick J. Bergin, M.D.
Michael J. Gitter, M.D.

(541) 747-1272
960 N. 16TH ST., STE. 104
SPRINGFIELD, OREGON 97477
Jay H. Chappell, M.D.
Richard C. Padgett, M.D.

(541) 484-1545
677 E. 12TH AVE., STE. N-540
EUGENE, OREGON 97401
Daniel G. Robinhold, M.D.
Jerold A. Hawn, M.D.
Leonard G. Christie, Jr., M.D.
Michael G. Antimisiaris, M.D.
James H. McClelland, M.D.

NAME Noll, Paul
ADDRESS _____ DATE 5/16/00
℞ Lipitor 10
Sig: 1 p.o. qD
200
30
☐ LABEL
REFILL 2 TIMES
_____ M.D.

Figure 8: doc-prescription.jpg

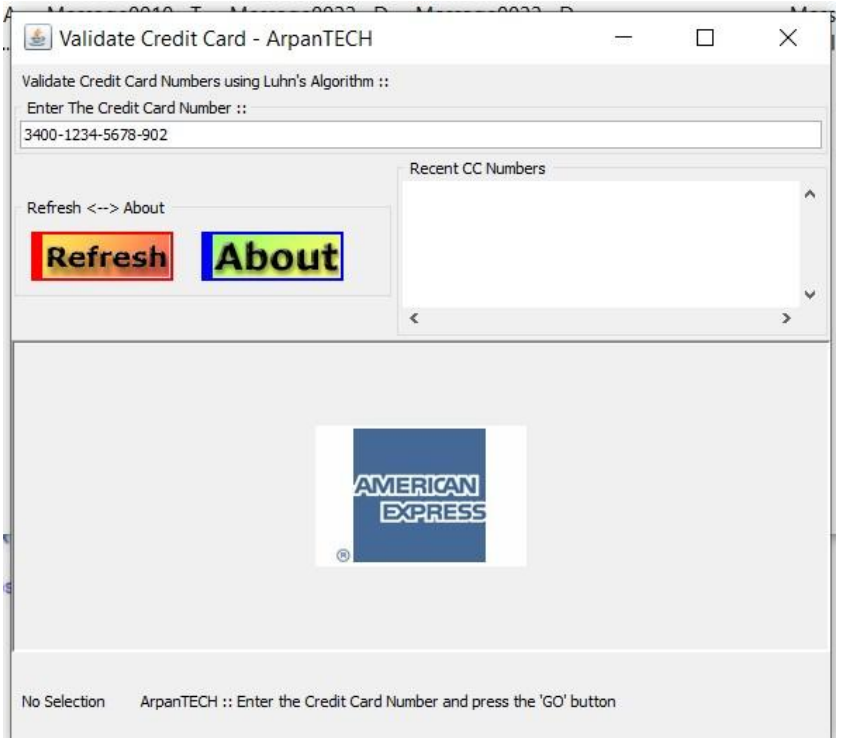
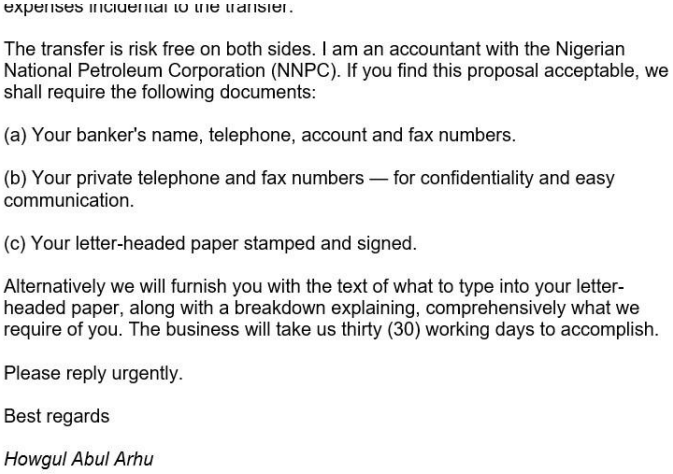


Figure 9: Software used to validate credit card number

	A	B	C
1	Dudes Name	What	$$$
2			
3	Little Timmy	Mth	$600.00
4	Big John	Special K	$250.00
5	John Washer	H	$250.00
6	Frank the Tank	H	$5,000.00
7	Sam I AM	Marijuana	$100.00
8	Mac Daddy	Special K	$200.00
9	Mr Freeze	Special K	$698.42
10	Methalotapus	Mth	$555.00
11	megamethamous	Mth	$250.00
12	Simple Simon	Marijuana	$698.00
13			

Figure 10: Various names associated with drugs



expenses incidental to the transfer.

The transfer is risk free on both sides. I am an accountant with the Nigerian National Petroleum Corporation (NNPC). If you find this proposal acceptable, we shall require the following documents:

(a) Your banker's name, telephone, account and fax numbers.

(b) Your private telephone and fax numbers — for confidentiality and easy communication.

(c) Your letter-headed paper stamped and signed.

Alternatively we will furnish you with the text of what to type into your letter-headed paper, along with a breakdown explaining, comprehensively what we require of you. The business will take us thirty (30) working days to accomplish.

Please reply urgently.

Best regards

Howgul Abul Arhu

Figure 11: Confidential Business Letter.doc : Scam attempt requesting personal informations

c. How do you investigate?

From the two images we need to investigate, we will find any files, documents, pictures, emails, or even words that look exactly the same from both of the images such as a person's name. From that particular word of interest, we will search thoroughly both of the images to find clues of the case.

From the content of images such as pictures and emails, we can come up with several keywords which are most likely connected to the pictures such as drugs or scam. This will allow us to search deeply for any hidden files that we might miss along with the normal search procedure.

Any encrypted documents or files we try to recover as much as we can for evidence and clues in the investigation. Weak encryptions (such as the password 'smack') are easy to overcome using dictionary attack to guess the right password. Strong encryptions (such as the password '0utt0st3a1 ') requires digging the drives for hints of the password.

d. How did the crime happen?

The criminal group seems to have been running its operations such as scamming and credit card theft for a while even before John Washer joined the group. Before that, John Washer and Wes Mantooth had planned an ATM theft on Thursday, July 12 2007. This can be seen in an email that Wes shared a ppt file of step by step of stealing a card from an ATM machine. With Rasco Badguy acting as the head of the group, they are actively engaging in scams and credit card stealing from July 2007 to August 2007. Methods that are used to steal credit card information are getting them from passprgram@aol, ATM hijacking, stealing

from unsuspecting people and scamming. John Washer on the other hand has been providing and selling drugs on his own even before joining the group.

On Wednesday June 20 11:56AM, John Washer Contacted Wes Mantooth about the "Special K" drug that he was looking for. From the conversation and pictures of prescription, they are involved in drug trafficking. The pictures that are hinting to this are doc-prescription.jpg and Prescription2.gif.

On Tuesday, 23 Jul 2007 12:59PM John Washer contacted Rosco Badguy with the help of Wes Mantooth. Later that day at 3:30PM, they exchanged AIM Mail contact to share passwords and avoid detection from the police. Rasco then shared some documents on how to steal credit card numbers to John and Wes. On 4:00PM that day John shows his deals with selling drugs in The Deals.doc to Rosco. On 27 Jul 2007 10:39AM, Rasco shared 2 credit card informations from Tom Smith and Bobby Jones by hiding them under document News Report.doc.

On Tuesday, July 24 2007 11:31AM, David introduces himself to John by sending a picture of his girlfriend. On August 01 2007 10:40AM, David shared his haul of credit cards from New York to John, John then shared his intent on a new source for debit card printing and sending Card_Printing_101.pdf. On August 01 2007 11:40AM, Rosco contacted John to share his card printers that make great licences and ID cards.

e. Discuss the scenario.

From the images, we learned that Wes Mantooth and Rasco Badguy are members of a criminal group running scams, drug selling, and credit card theft. Before John Washer was involved in Wes's group, he and Wes had planned out an ATM theft by stealing the target credit card at the ATM machine. After that, Wes introduces John Washer to join the group. From there, the three of them discuss and share various methods of getting profit through crimes such as ways to steal credit card numbers and drugs. To avoid detection from the police, they exchange passwords through another channel called AOL Network Screen Name and use its service AIM Mail. Rasco acts as a mastermind for any operation in the group and provides guides and tools. David Thomas, also known as the 'Skimmerman' excels at printing cards using stolen credit card information and providing tools for the group. In the end, Rasco and John got to meet for a fishing trip "in the mountains". This can be seen from one of the emails shown John giving detailed directions to Rasco about their meeting spot.

f. Is there any relationship between both images provided? If yes, discuss.

Yes, John Washer kept some of the records of his work with the group that he wishes to be hidden from the police in his thumb drive. Other than that, one ppt file can be identified from both of the images named ATM_THEFTS1.ppt. From one of the images which is Thumbdrive.E01, one of the files stated John Washer has owes $250.00 and from the second image named Washer.E01, John Washer's name appears actively especially in email. Wes' portrait also can be identified in the Thumbdrive.E01 which also actively using email in the other image.