



Presents



Scammer!

The “Roger” Report

Help prevent scams and fraud.

Please share this with everybody!

The more people who read this report, the fewer the number of people who will fall for this type of scam in the future.

You have probably heard of the “Microsoft scam”, where you receive a telephone call from someone purporting to be from Microsoft who tells you that your computer is infected. The caller tells you that it is necessary for you to have your computer cleaned immediately, a service he is happy to provide for a small fee. He can do this by remotely logging into your computer.

Of course, Microsoft NEVER calls users to inform them that their computer is infected. If you grant the caller access to your computer, he will likely infect your computer with malicious software designed to capture information enabling him to access your bank account and charge cards, and do anything else he desires.

Recently, I received a call from “Roger” who works at “Technical Department”.

Roger: “Your computer is infected, you need to clean it right away.”

Me: “Oh no, that doesn’t sound good, what should I do?”

Roger: “No problem sir, I can take care of it for you from remote”.

Of course, my computer was not infected. The only one that might call you to tell you that your computer is infected is your Internet provider, and they won’t offer to fix it for you from remote. They will tell you to take it to a professional computer shop (like McLean Micro) and have it properly fixed.

Fortunately, I had a virtual machine ready that I could grant him access to. If you don’t know what a virtual machine is, it is a fake computer that runs in a window on your real computer. It runs its own copy of Windows, and can be completely isolated from the real computer.

I was able to observe everything he did, and capture video and screen shots. And since I am a computer/network technician at McLean Micro (and pretty good at my job), I was able to fool “Roger” and make him believe what I wanted him to.

During our remote sessions (which spanned several weeks), “Roger” often

put me on hold to consult with his “senior technician”, or his “accounts manager”.

When he “puts me on hold”, I’m not really on hold, I can hear what is going on at the “technical center”. It sounds like there are many people working there, under the direction of one or more supervisors.

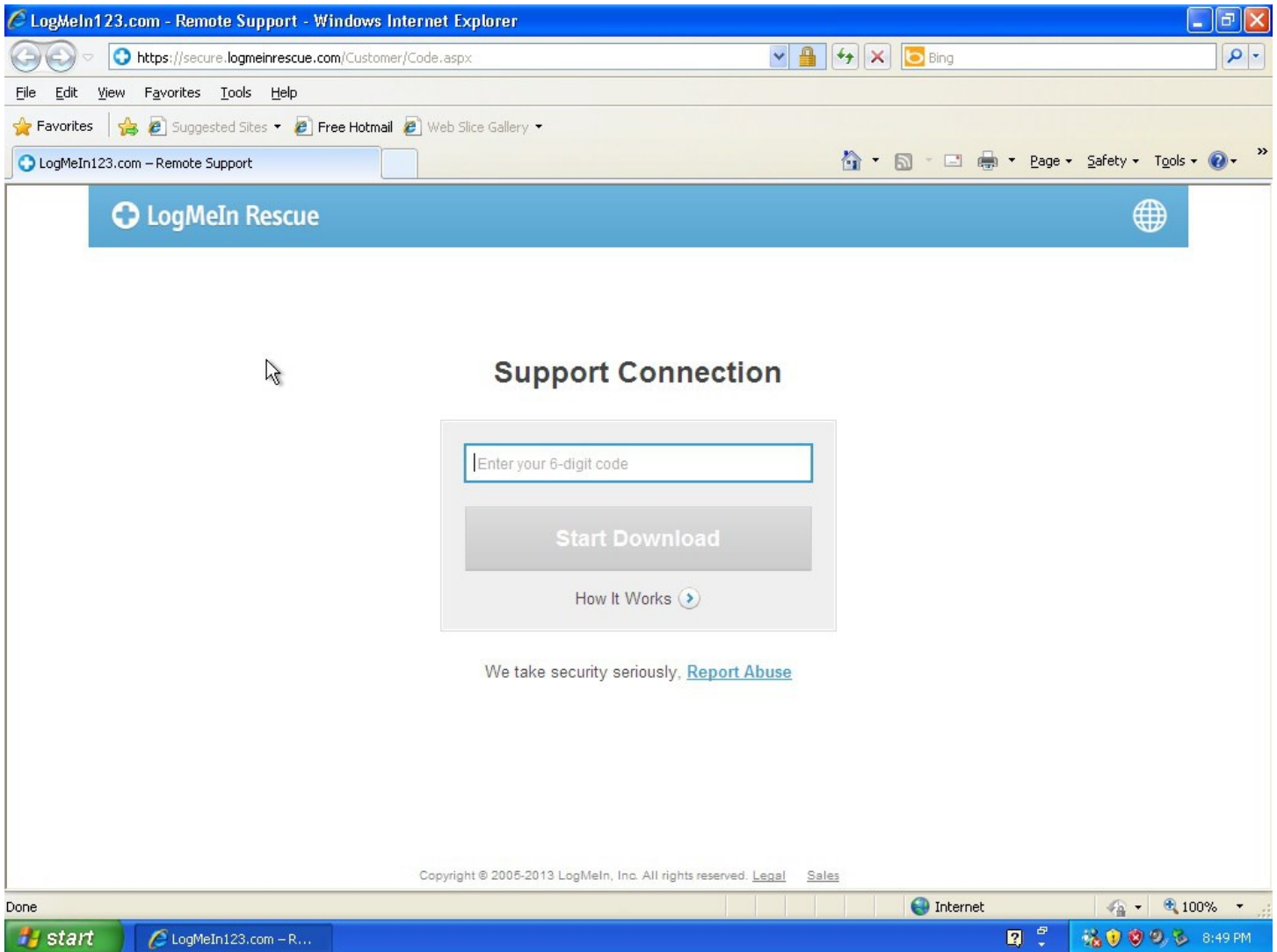
It is obvious that “Roger” is working from a script, and when anything happens that he doesn’t know how to deal with (for example, when the “customer” doesn’t have a charge card), he asks someone else what he is supposed to do. “Roger” appears to have little technical skill, and he (and his superiors) are easily fooled.

You might ask why I would want to bother wasting my time with “Roger” instead of just hanging up. There are a number of reasons:

- I wanted to see exactly what these scammers do when they access your computer from remote.
- When they are trying to scam me, they aren’t scamming someone who is unable to spot and deal with this type of scam.
- I may be able gather information that could be of help to law enforcement in preventing this type of scam in the future (or, as was the case here, try to help someone being scammed right now).
- It can be fun to outsmart a scammer like “Roger”, there were a couple of times when I had to cover the mouthpiece on the phone, so he wouldn’t hear me laughing.

If you’re going to try to scam someone who is smarter and more technically competent than you are, you aren’t going to win. Just ask “Roger”.

Note that when I refer to “Roger”, I am referring not only to the voice I hear on the phone, but to the person or persons who are accessing my computer from remote. I believe that the “Roger” I hear on the phone is merely the voice the victim hears, and that much of the remote work is done by someone else.

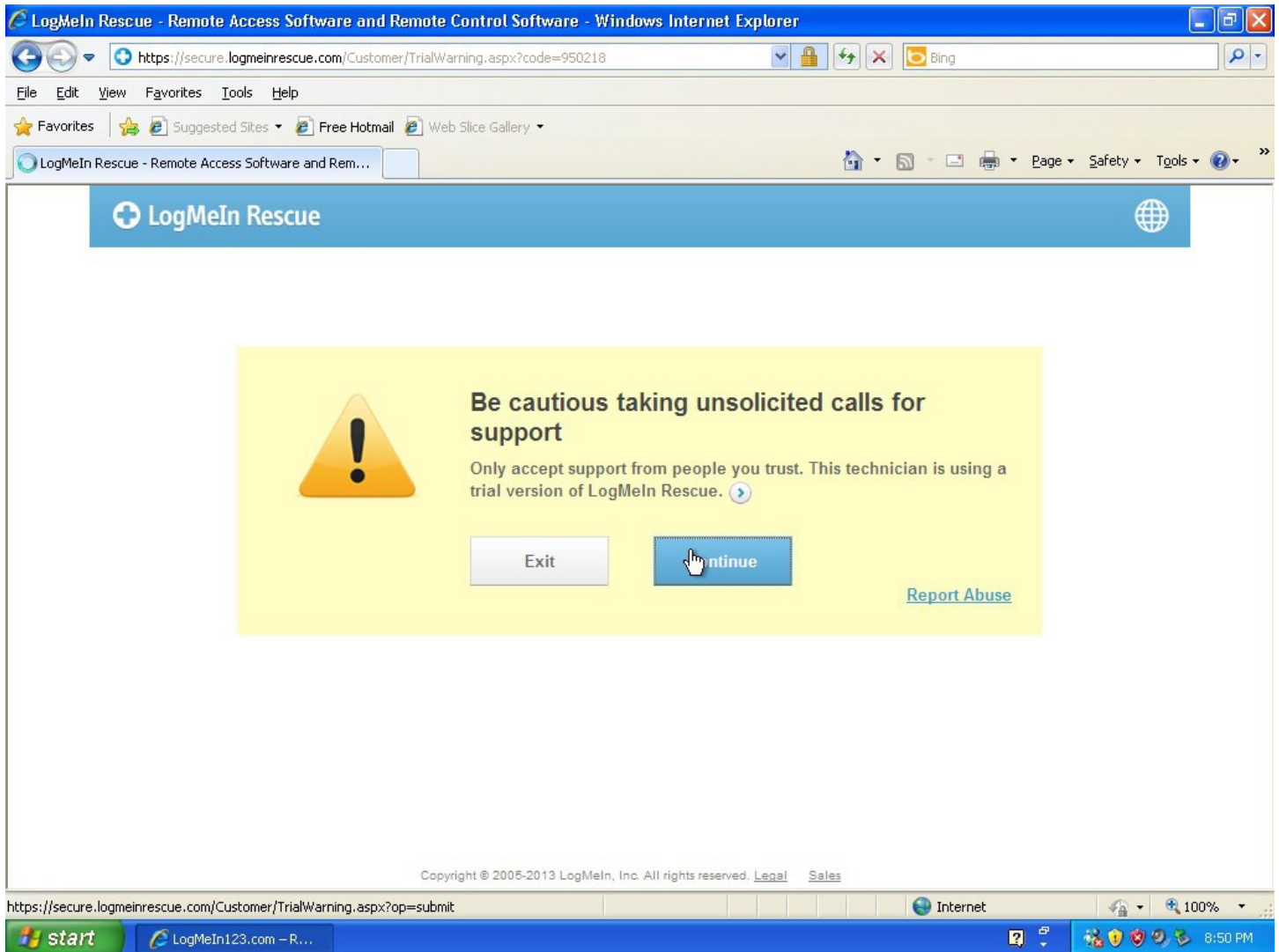


Session One

The first thing a scammer needs is access to your computer. “Roger” directed me to a site, secure.logmeinrescue.com, where I would download a utility granting “Roger” remote access to my computer.

Since I had a virtual machine ready, that is what I granted him access to.

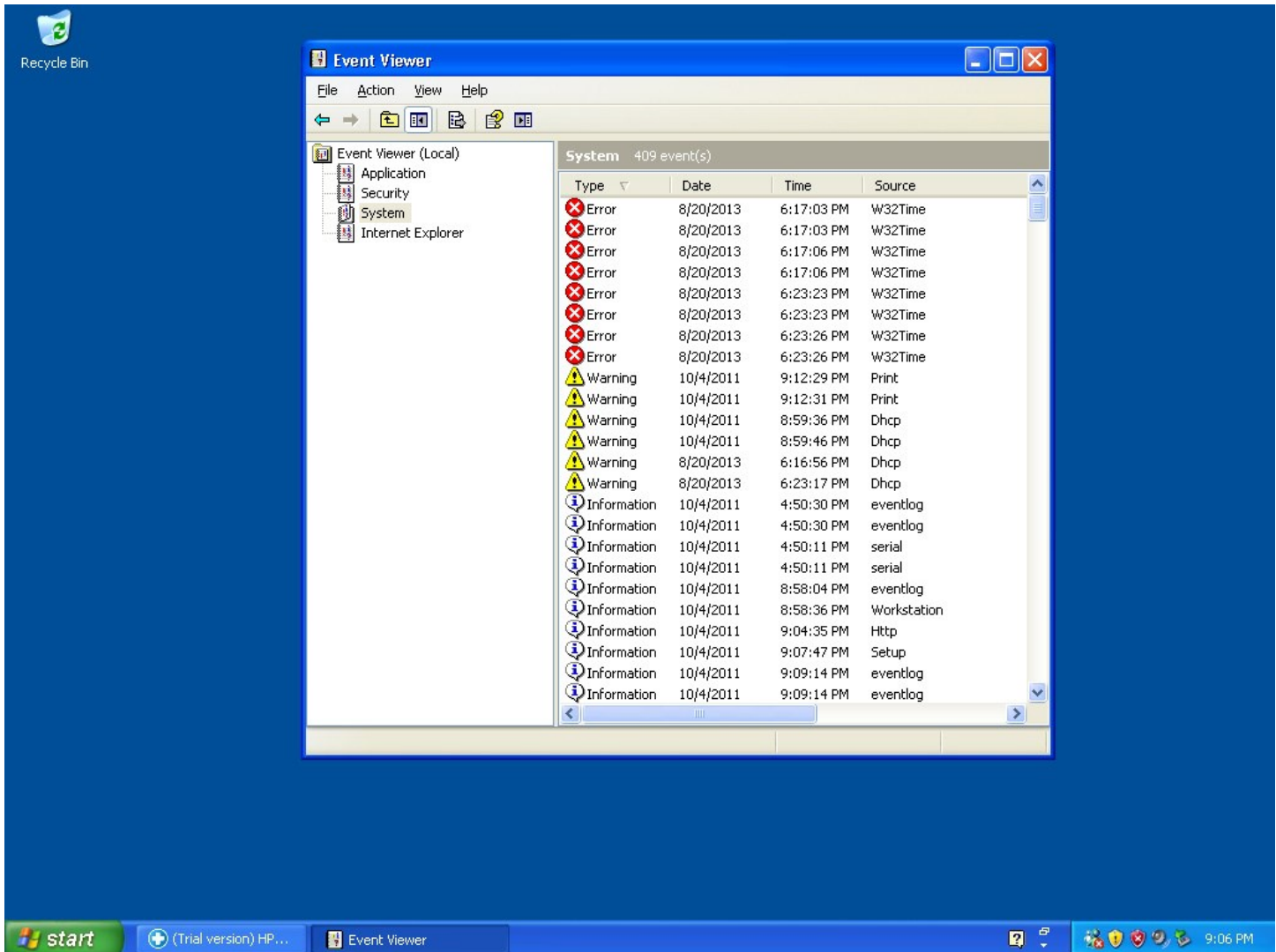
To clarify, the sections “Session One” or “Session Two” etc, are not consecutive days, and they are not my only phone conversations with “Roger”. They are only days when I allowed him remote access to my “computer”.



I didn't ask "Roger" about the warning that popped up when I ran the remote access utility, I didn't want to ask him too many questions he couldn't answer.

If he knew he wasn't scamming me, he would have disconnected.

LogMeInRescue is a legitimate service that allows IT people to log into their clients computers from remote to fix minor issues. It can also be used by scammers to access your computer, **but only if you let them.**

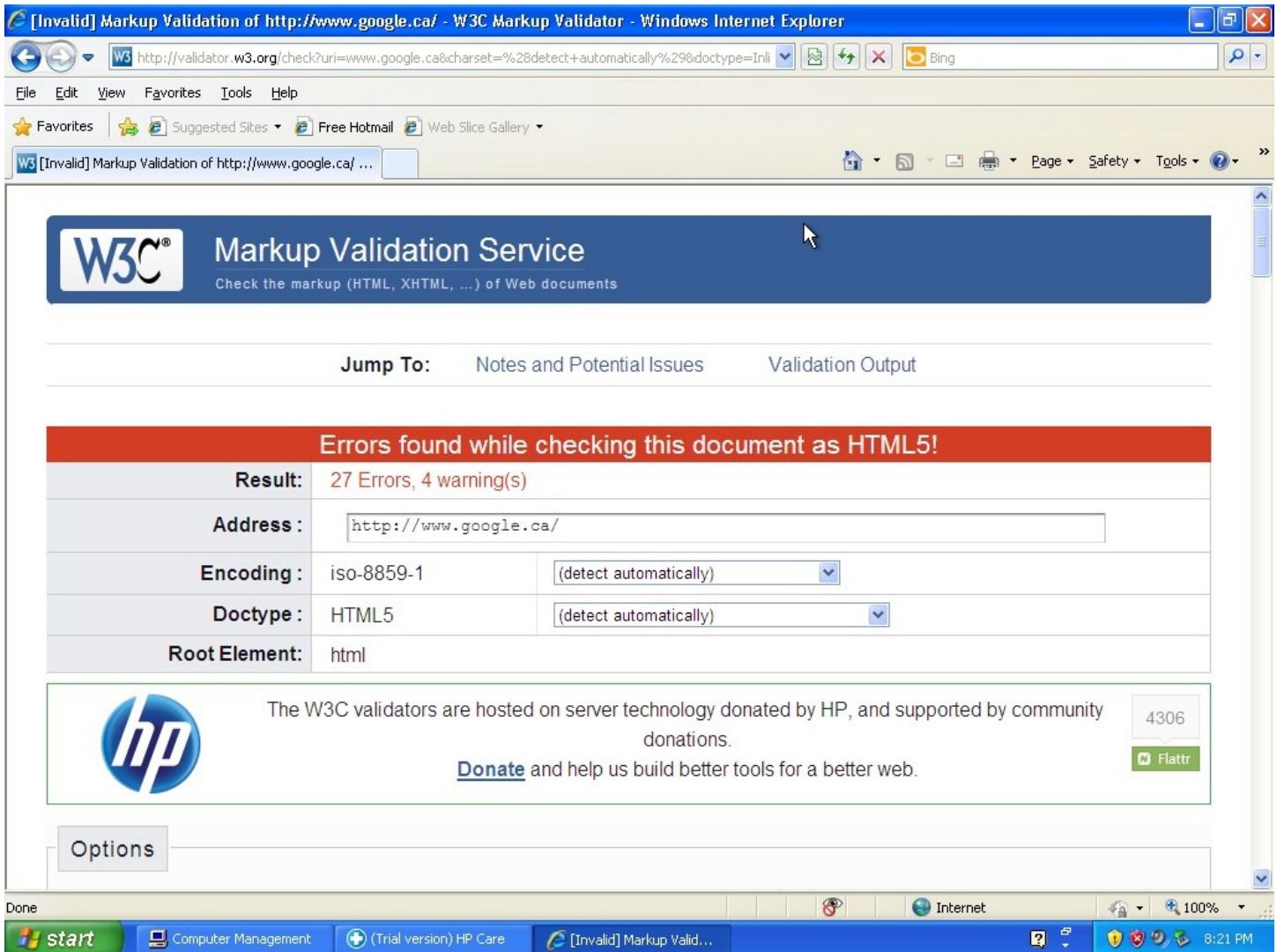


“Roger” opened my event viewer and explained that the red errors were caused by viruses and infections.

Roger: “Each of these red and yellow marks are thousands of infections, this is bad. Very very bad.”

In reality, the virtual machine was a fresh install. A certain number of errors and warnings in the event logs are normal (depending on the error or warning) and there was nothing wrong with the computer.

Note in the taskbar that the remote access software is the trial version of HP Care (which uses LogMeInRescue).



The screenshot shows the W3C Markup Validation Service interface in Internet Explorer. The browser title is "[Invalid] Markup Validation of http://www.google.ca/ - W3C Markup Validator - Windows Internet Explorer". The address bar shows the URL "http://validator.w3.org/check?uri=www.google.ca&charset=%26detect+automatically%29&doctype=Inli". The page content includes the W3C logo and the text "Markup Validation Service Check the markup (HTML, XHTML, ...) of Web documents". Below this, there are tabs for "Jump To: Notes and Potential Issues Validation Output". A red banner reads "Errors found while checking this document as HTML5!". A table below the banner shows the following details:

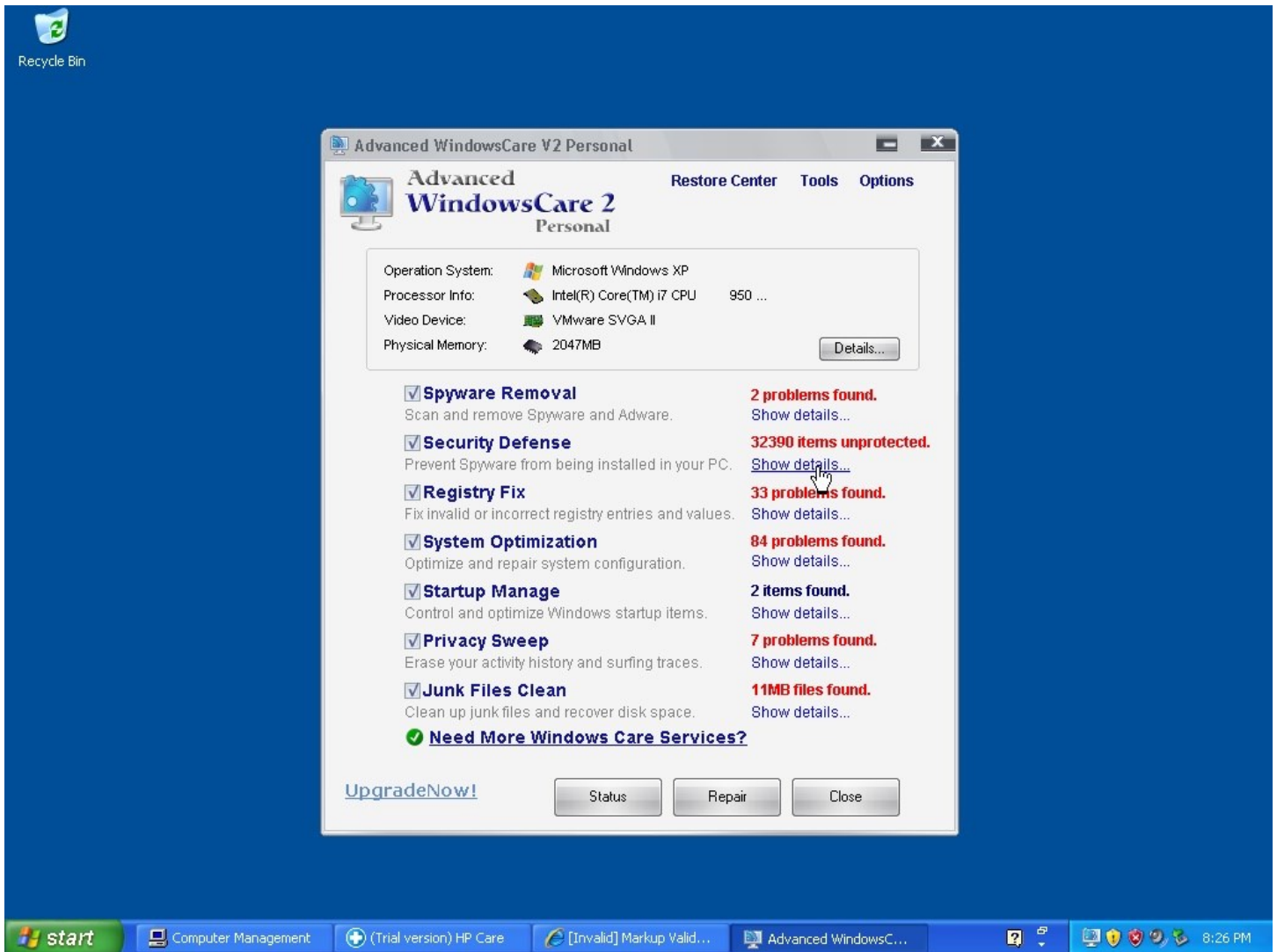
Result:	27 Errors, 4 warning(s)	
Address :	<input type="text" value="http://www.google.ca/"/>	
Encoding :	iso-8859-1	<input type="text" value="(detect automatically)"/>
Doctype :	HTML5	<input type="text" value="(detect automatically)"/>
Root Element:	html	

Below the table, there is an HP logo and text: "The W3C validators are hosted on server technology donated by HP, and supported by community donations." A "Donate" link is present, along with a "Flattr" button and the number "4306". At the bottom, there is an "Options" button. The Windows taskbar at the bottom shows the start button, "Computer Management", "(Trial version) HP Care", and the active window "[Invalid] Markup Valid...". The system tray shows the time as 8:21 PM.

Next, “Roger” opened my browser (Internet Explorer) and went to an HTML validation page. He entered the Google home page in the validator, which generated a number of errors and warnings.

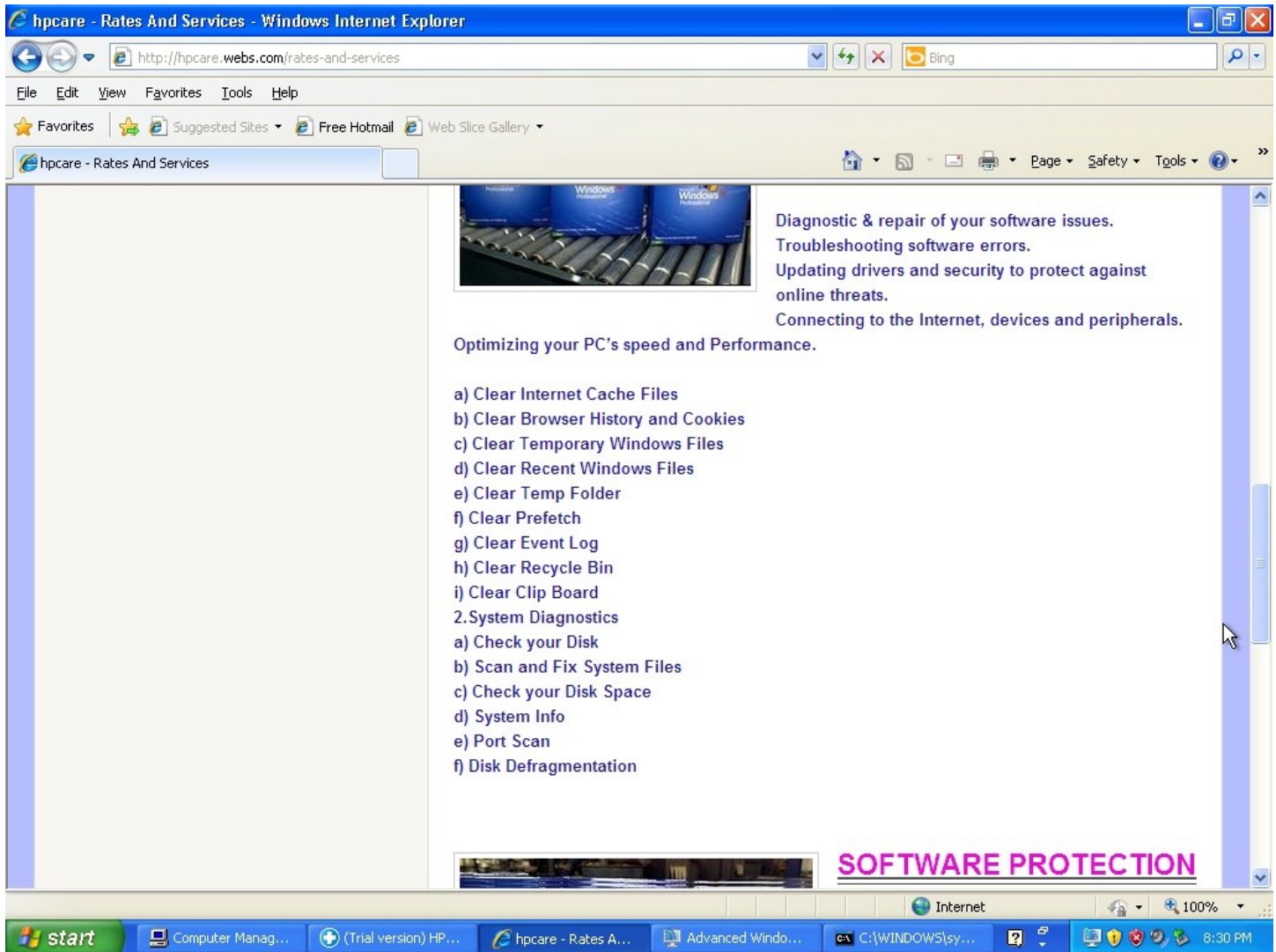
These, he explained, were further indications of the severity of the infections in my computer.

Obviously, any HTML errors on the Google home page have nothing whatsoever to do with my computer. I didn’t ask “Roger” about this, I was pretending to be technically challenged, so played along to see what would happen next.



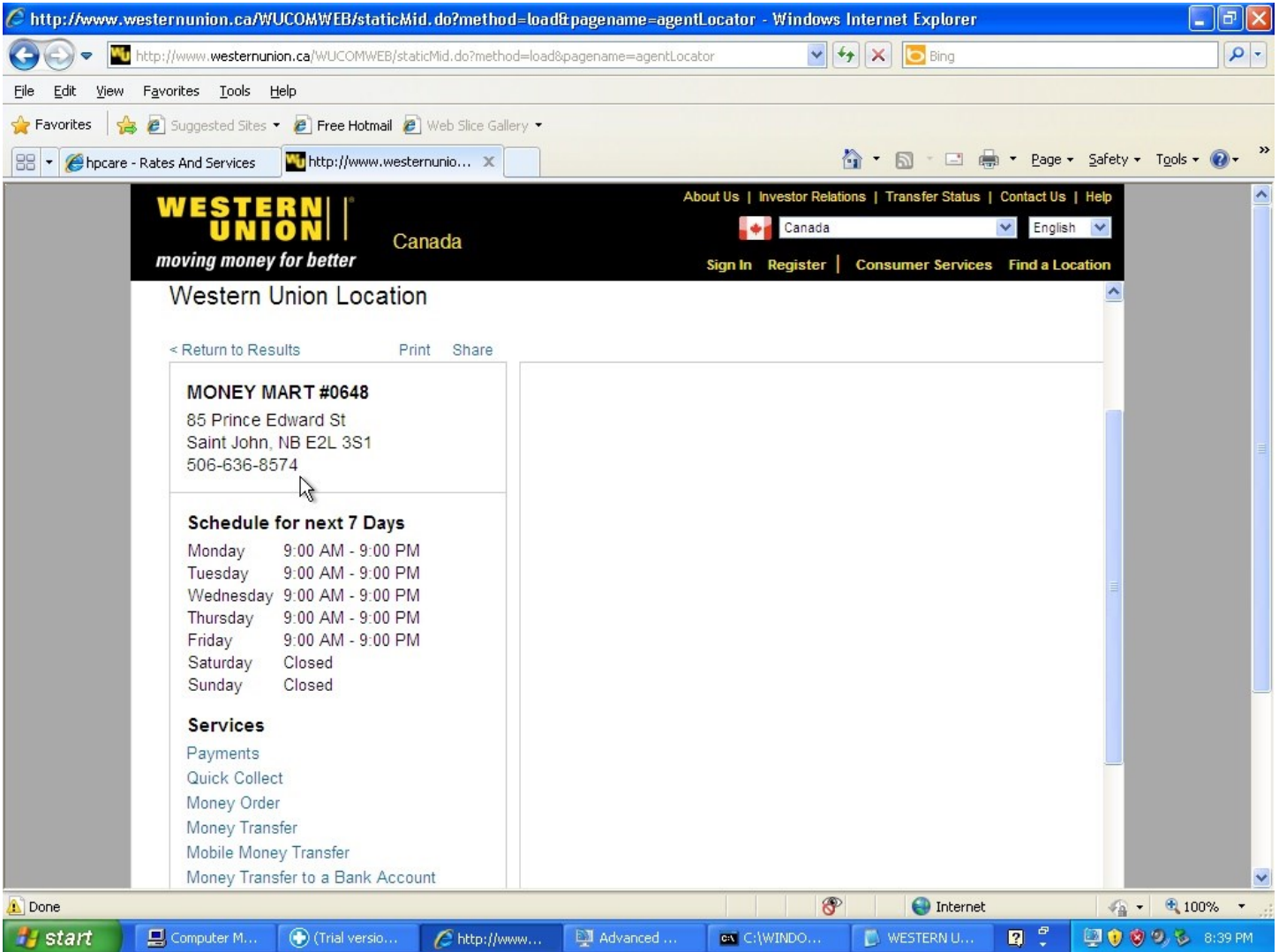
Now “Roger” transfers software to my computer, and installs and runs it.

I have never heard of “Advanced WindowsCare 2”, but I do know that a fresh install of Windows isn’t going to have thousands of problems. The virtual machine I allowed “Roger” to access had never even been on the Internet, except to activate the Windows.



After poking around my system for a few minutes, including looking at my system properties, and doing some useless things at a command prompt (no doubt to convince me of the level of infection on my computer and of “Roger’s” ability to correct them), we wind up at a page where I can purchase “services” to fix my system.

These “services” include (among other things) emptying my recycle bin, and clearing my clip board, all for the bargain price of \$199. And it even includes lifetime support! But as you will see later, **if you fall for the scam, they may be able to steal far more than the initial payment from you, and do so without any further help from you.**



The screenshot shows a Windows Internet Explorer browser window displaying the Western Union website. The address bar shows the URL: <http://www.westernunion.ca/WUCOMWEB/staticMid.do?method=load&pagename=agentLocator>. The page title is "Western Union Location". The main content area displays the following information:

WESTERN UNION Canada
moving money for better

Canada (dropdown menu) English (dropdown menu)

Sign In Register Consumer Services Find a Location

Western Union Location

< Return to Results Print Share

MONEY MART #0648
85 Prince Edward St
Saint John, NB E2L 3S1
506-636-8574

Schedule for next 7 Days

Monday	9:00 AM - 9:00 PM
Tuesday	9:00 AM - 9:00 PM
Wednesday	9:00 AM - 9:00 PM
Thursday	9:00 AM - 9:00 PM
Friday	9:00 AM - 9:00 PM
Saturday	Closed
Sunday	Closed

Services

- Payments
- Quick Collect
- Money Order
- Money Transfer
- Mobile Money Transfer
- Money Transfer to a Bank Account

Me: "But Roger, I don't have a charge card, what can I do?"

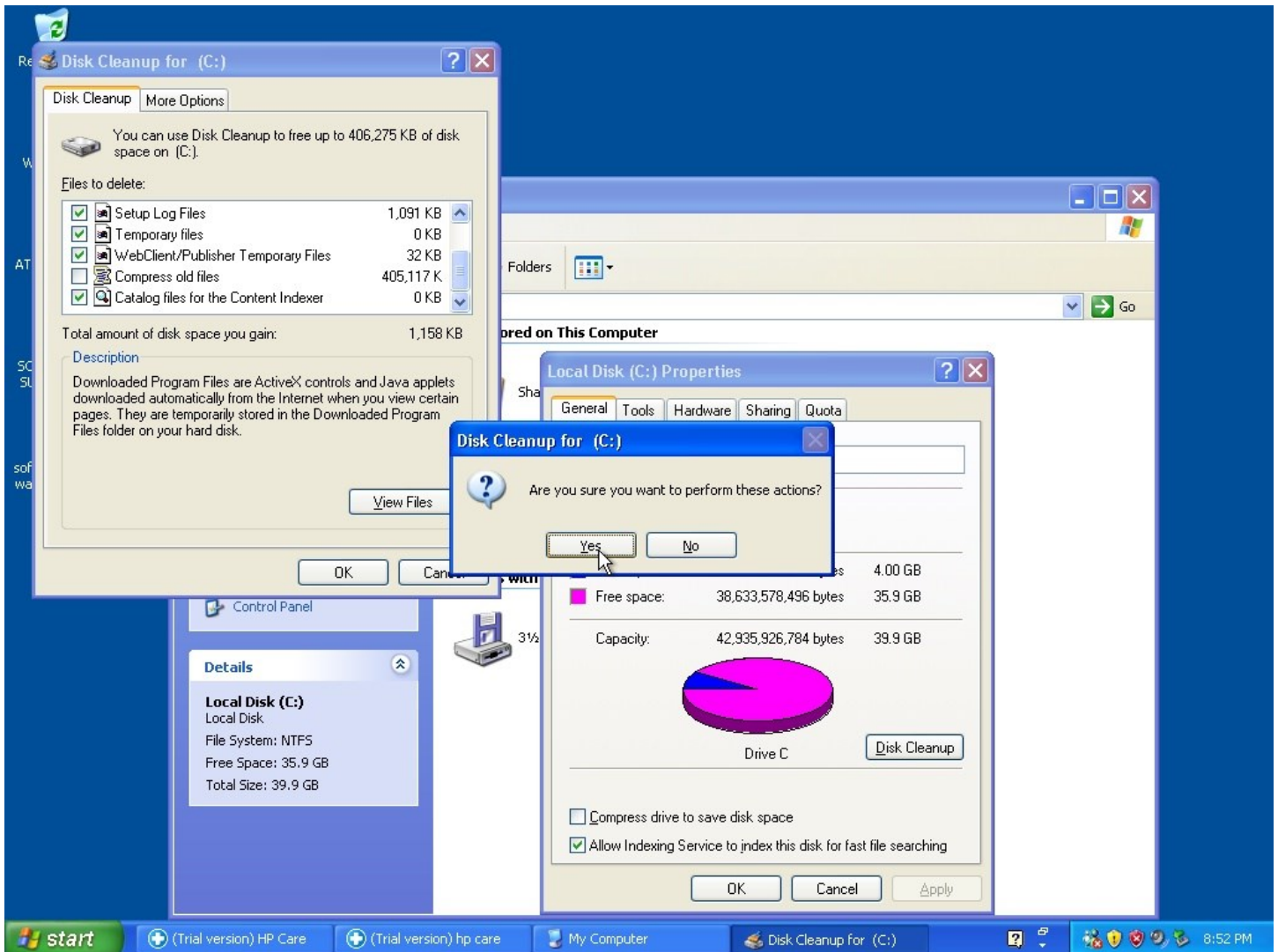
Roger: "Let me put you on hold while I talk with my accounts manager."

...

Roger: "Ok, I need you to go to Western Union, and send a money transfer."

Payment will be made to the "accounts manager". Accounting, he explained, has been "outsourced to India", so that is where I will have to send the payment.

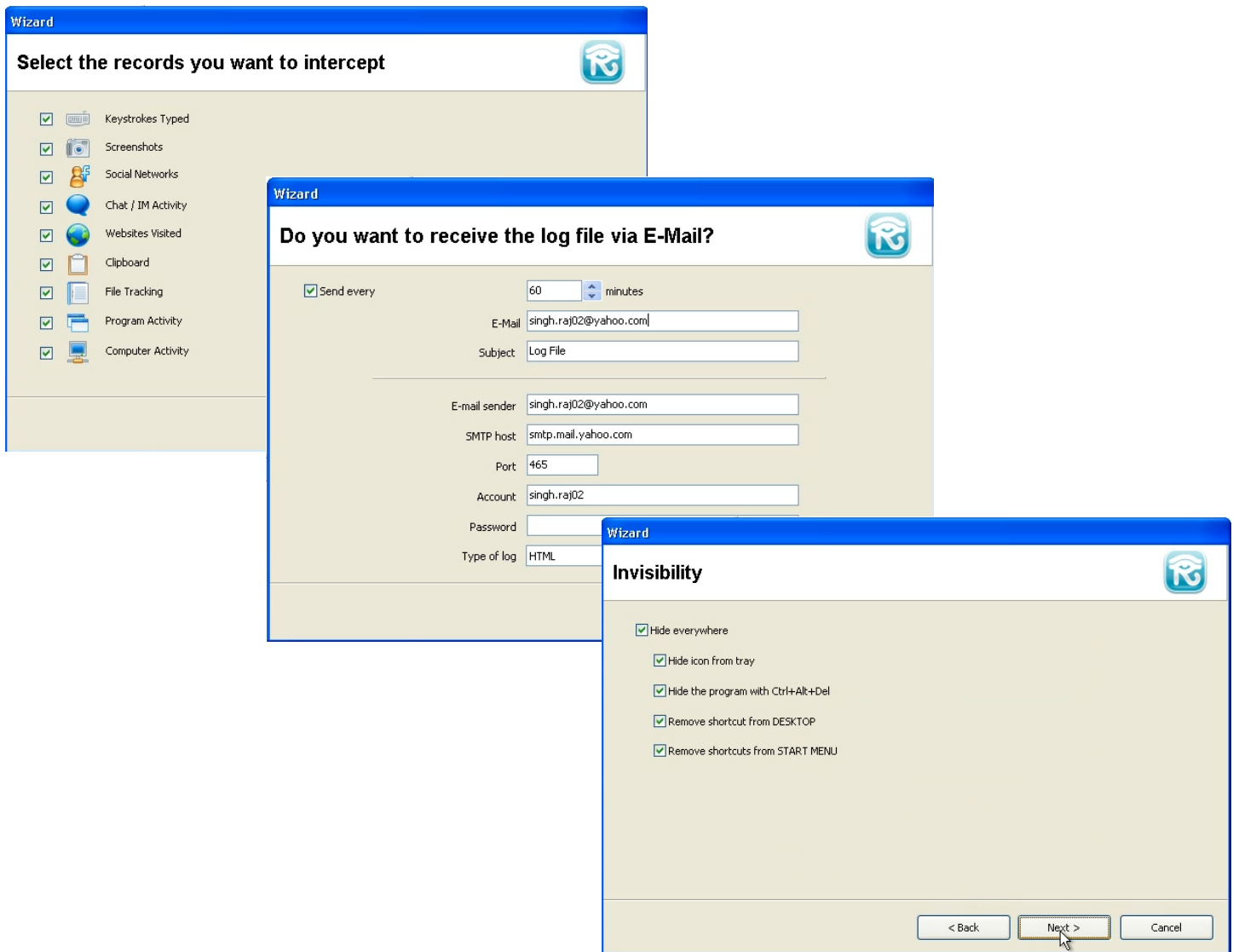
"Roger" trusts me, so he will begin the service immediately.



“Roger” installs more software on my system, then does a disk defragment (which runs very quickly in a virtual machine), and runs the disk cleanup wizard.

“Roger” doesn’t need me at this point, so we hang up while “Roger” continues to work from remote.

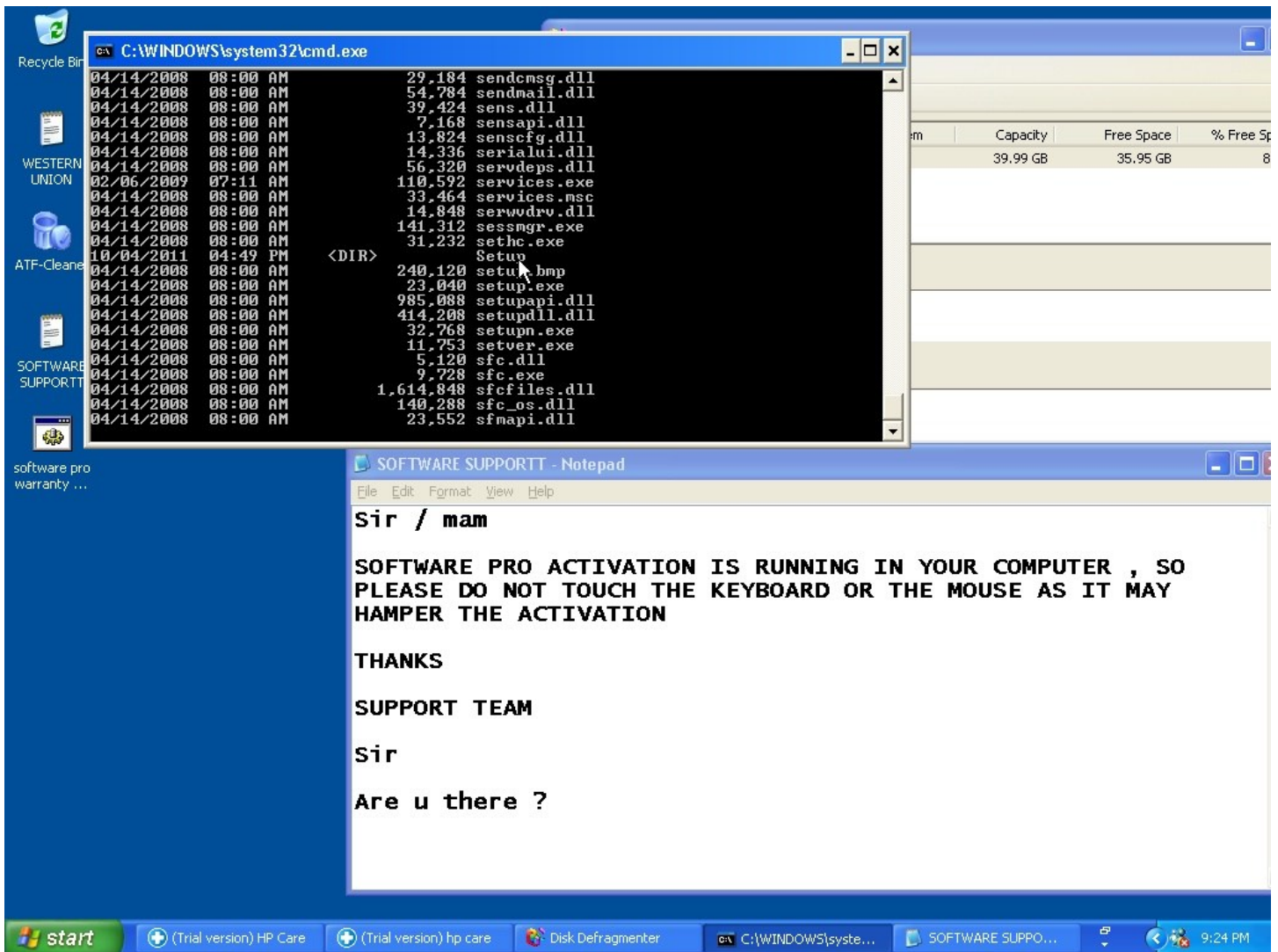
I told him I was going to bed, but of course I was watching (and recording) everything he did.



Now “Roger” installs software that will monitor everything anyone does on the computer. It reads every key you type, records every web site you visit, every file you open, and everything else you do.

He sets it to email the log file every 60 minutes, and to hide in the system so it is undetectable.

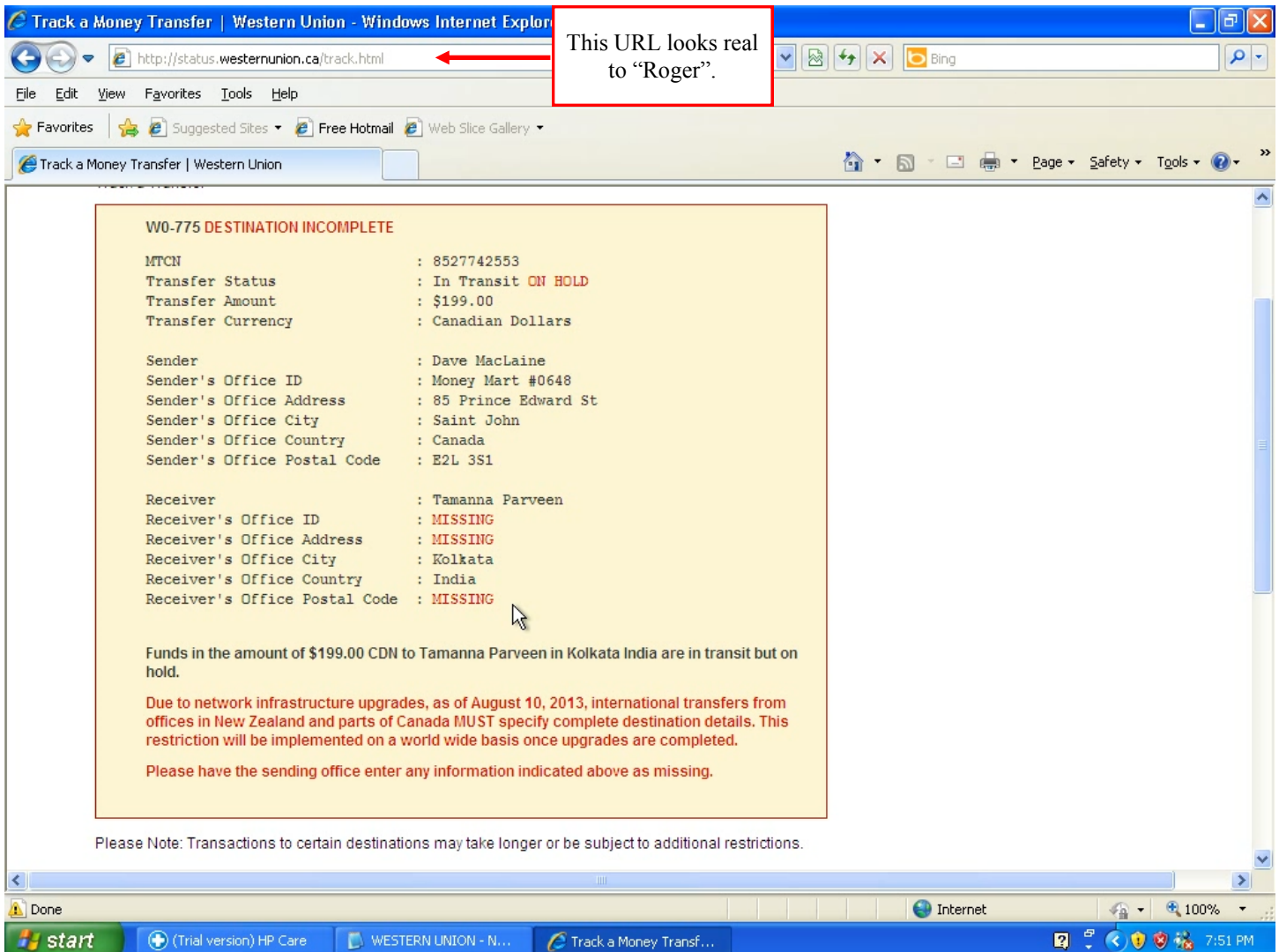
Using this, “Roger” can capture banking and charge card information, passwords, and everything else that is done on the computer. He can (and will) use this information to steal money from the victim’s charge card and/or bank account.



“Roger” downloads and runs “Software Pro Activation” on my computer. He explained before that he will install this to help fix my computer, and I should not touch the keyboard or mouse. He puts a note on the screen to this effect.

In reality, “Software Pro Activation” is just a batch file that keeps a directory listing scrolling by forever in a DOS window. Apparently, “Roger” wants the computer to look like it is doing something useful, so I will think he is hard at work earning his money (which, or course, he will never receive).

This runs for a long time. After a while, “Roger” shuts down the computer. He said he would do this when he was done for the night.



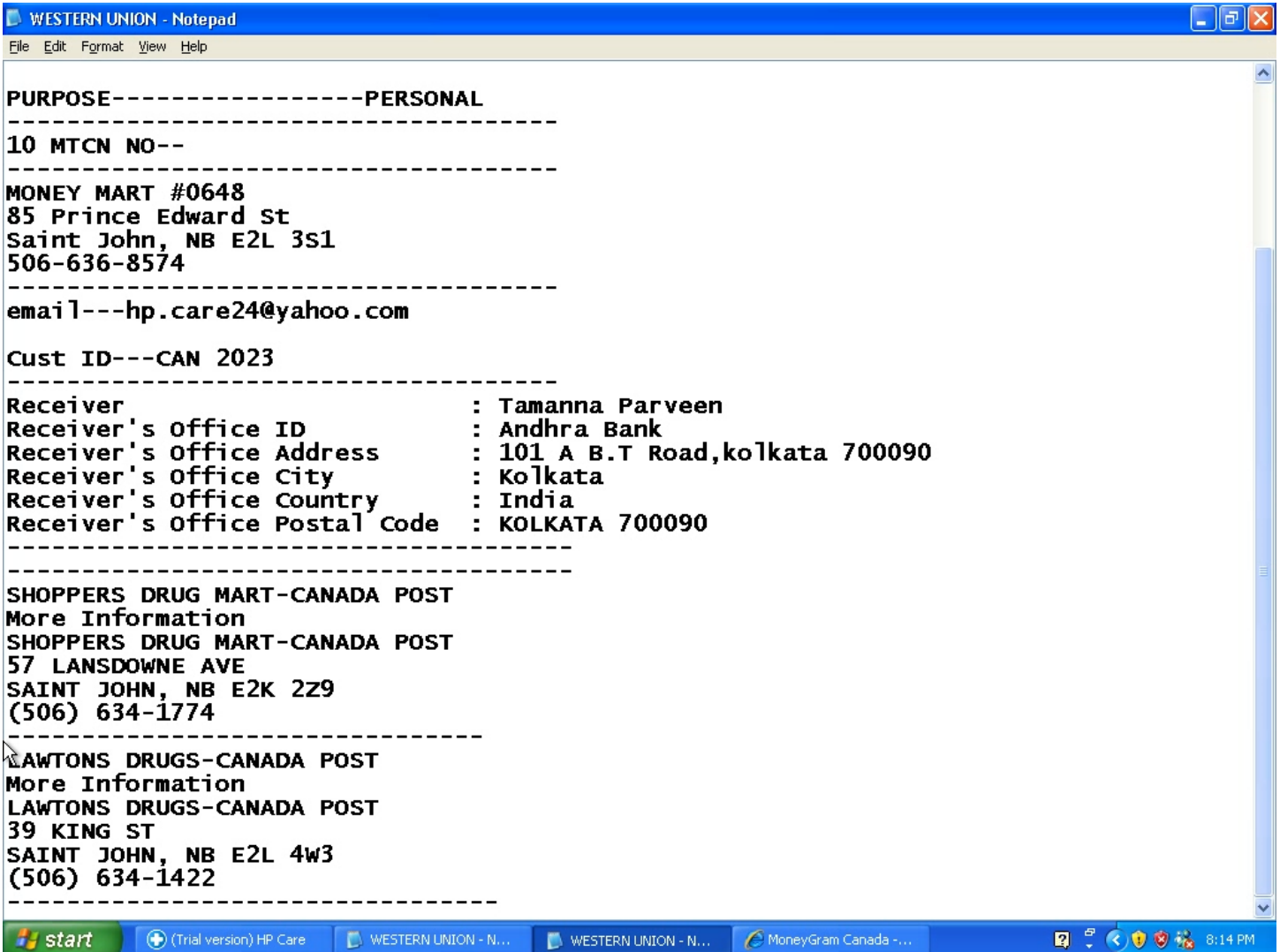
Session Two

When “Roger” called the next day, I was again ready for him.

Me: “The girl at Western Union said that because of a new network system they have in Canada, I need to tell them more information about where your accounts manager will pick up the money.”

Roger: “Ok, let me put you on hold while I check with my accounts manager.”

Note the URL above, it appears to point to a valid Western Union page. **Actually, it is a fake page on my web server running at home.** You can do this type of thing if you are a network technician and run your own web and DNS servers.



```
WESTERN UNION - Notepad
File Edit Format View Help

PURPOSE-----PERSONAL
-----
10 MTCN NO--
-----
MONEY MART #0648
85 Prince Edward St
Saint John, NB E2L 3S1
506-636-8574
-----
email---hp.care24@yahoo.com

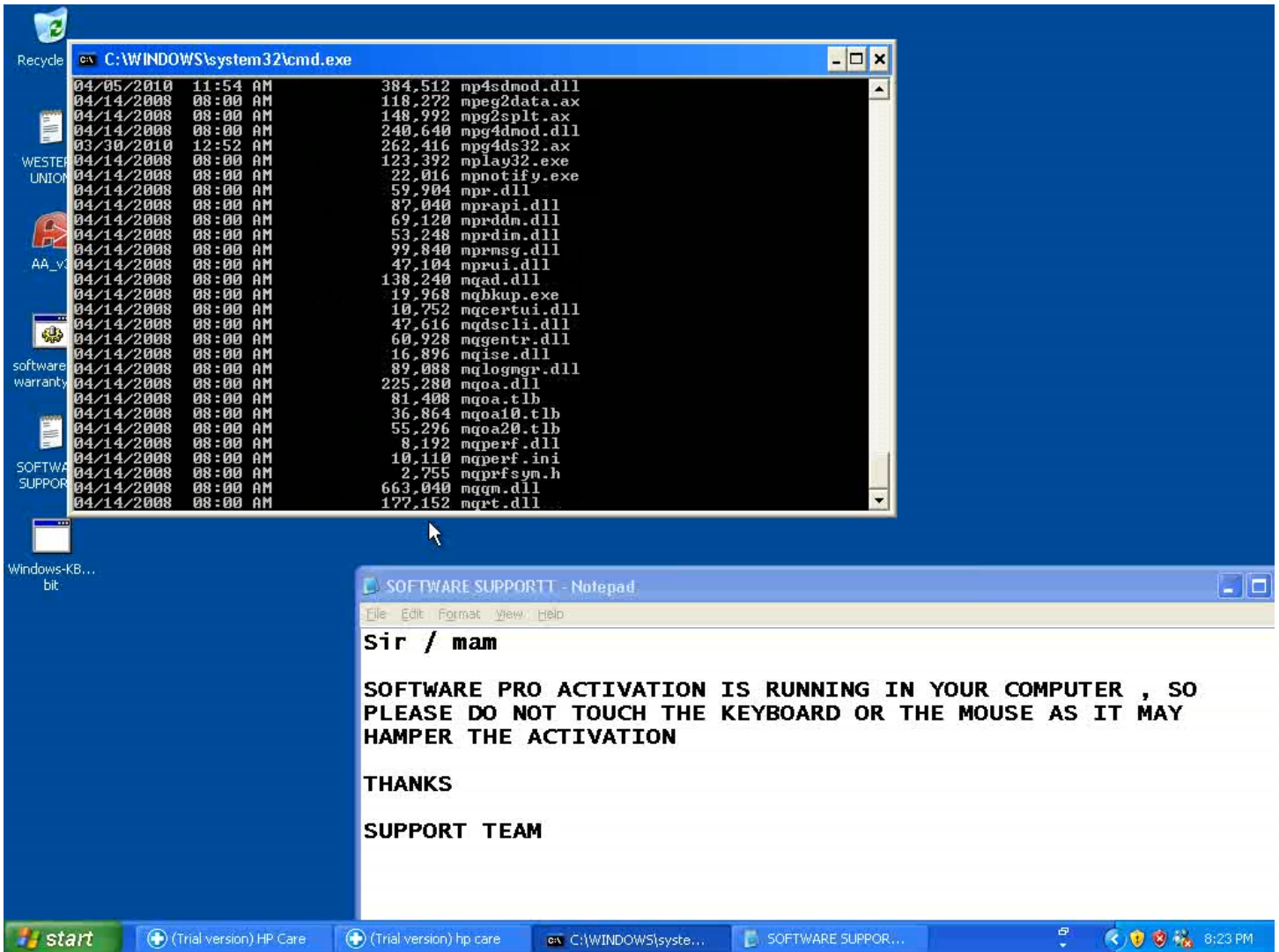
Cust ID---CAN 2023
-----
Receiver                               : Tamanna Parveen
Receiver's Office ID                   : Andhra Bank
Receiver's Office Address               : 101 A B.T Road,kolkata 700090
Receiver's Office City                 : Kolkata
Receiver's Office Country              : India
Receiver's Office Postal Code         : KOLKATA 700090
-----
SHOPPERS DRUG MART-CANADA POST
More Information
SHOPPERS DRUG MART-CANADA POST
57 LANSDOWNE AVE
SAINT JOHN, NB E2K 2Z9
(506) 634-1774
-----
LAWTONS DRUGS-CANADA POST
More Information
LAWTONS DRUGS-CANADA POST
39 KING ST
SAINT JOHN, NB E2L 4W3
(506) 634-1422
-----

start (Trial version) HP Care WESTERN UNION - N... WESTERN UNION - N... MoneyGram Canada - ... 8:14 PM
```

“Roger” agrees to provide the required information, and opens notepad to type it in. He tells me to be sure to go back to the Western Union office tomorrow with the information, and complete the transfer.

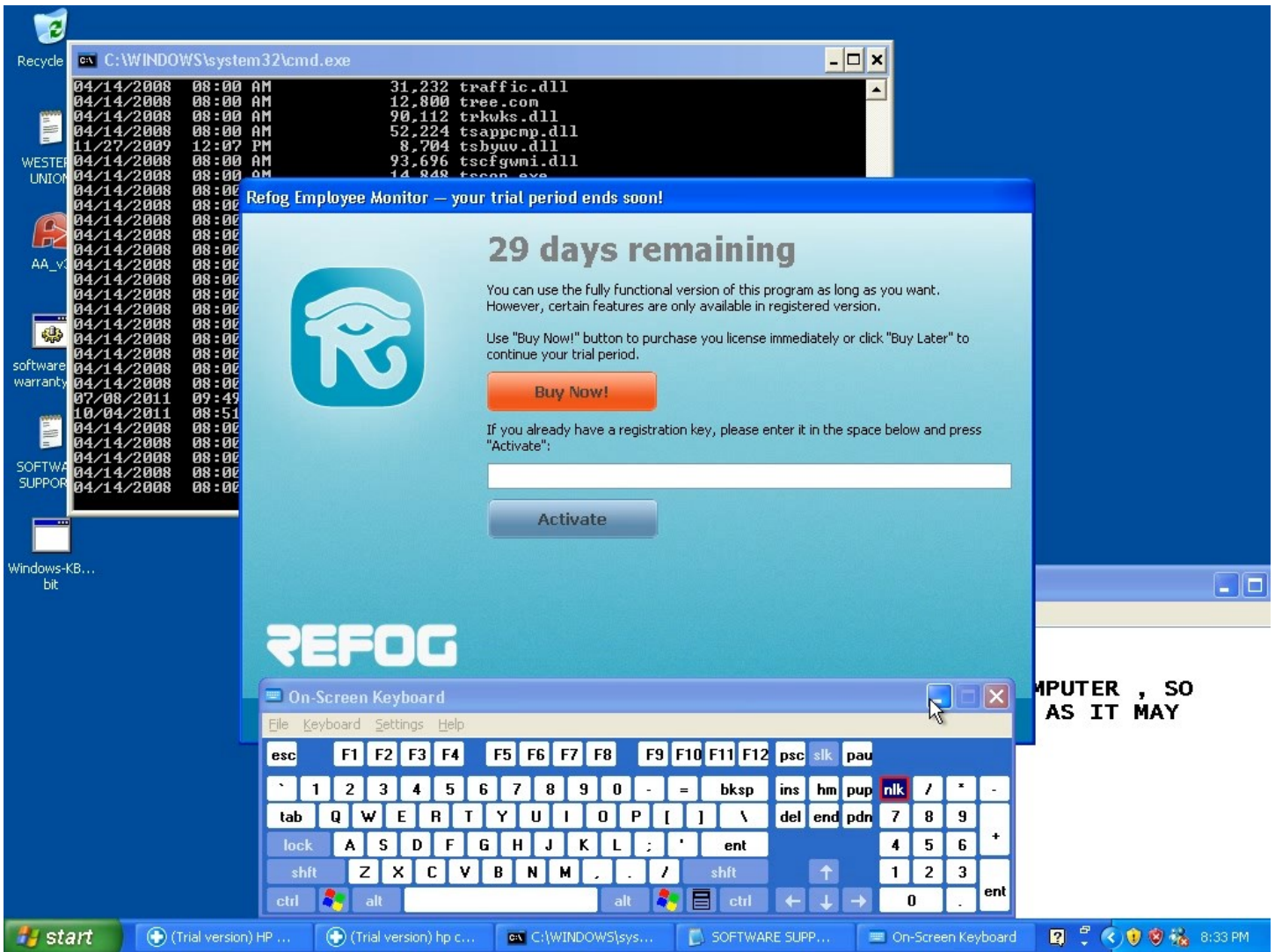
He says that if there is any problem with Western Union, to send a MoneyGram instead, and he finds two locations (the post offices in Shoppers Drug Mart and Lawton Drugs) where I can do this.

He explains that I should tell them the transfer is for personal (not business) reasons “to save on the money transfer fee”. I thank “Roger” for trying to save me some money. While doing my best not to laugh, I tell him I will take care of it in the morning.



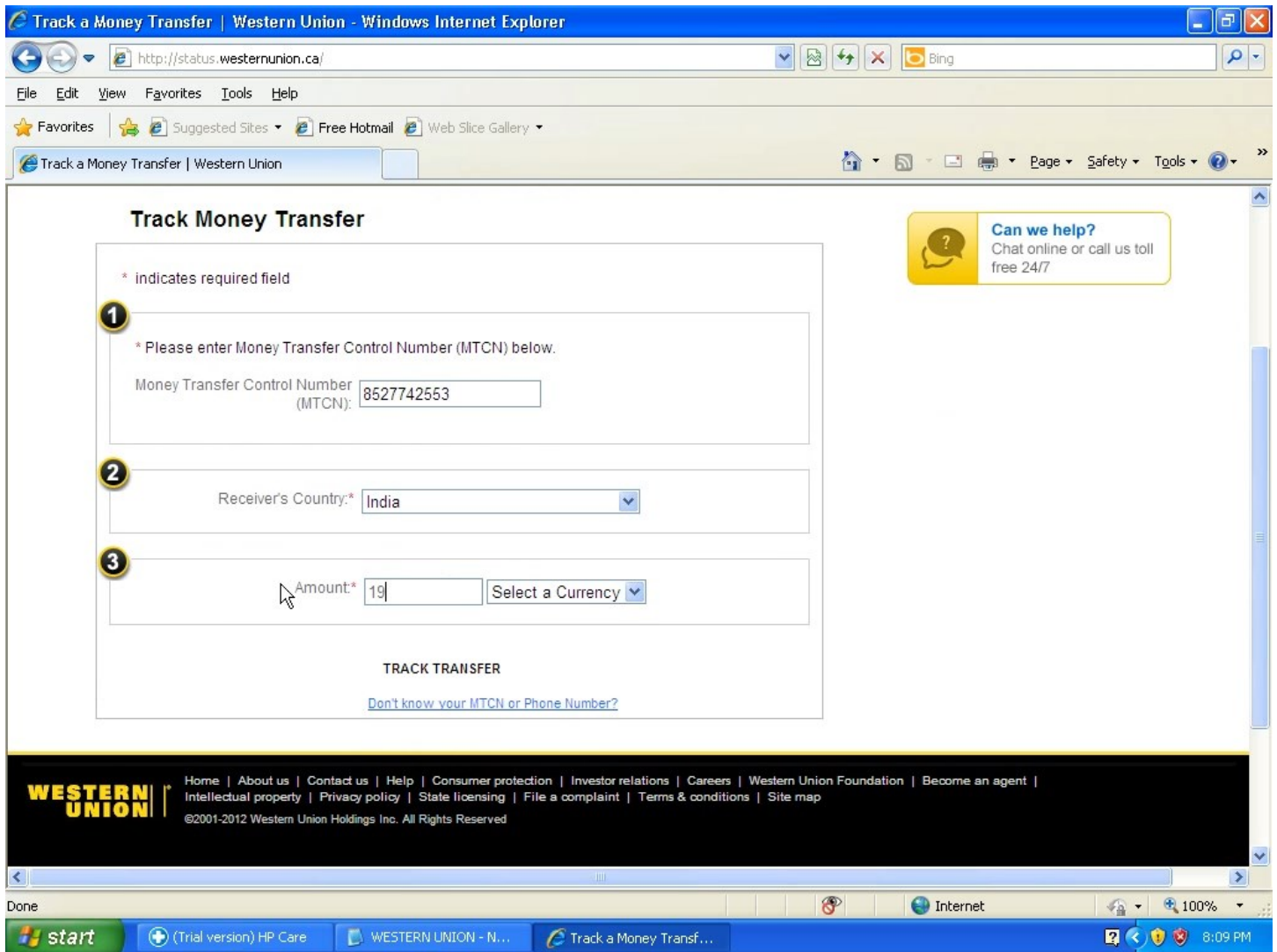
I hang up with “Roger”, because he does not need me on the phone as he works from remote, and I tell him I am going to bed.

He runs “Software Pro Activation” again. The directory listing scrolls by endlessly.



“Roger” double checks the remote spy software he previously installed (a trial version of employee monitoring software) to see what I have done between calls. I didn’t even power on the virtual machine, so there is nothing to report (which is why he didn’t get any email from the software).

He then does all the same things he did the previous night, and shuts down the computer when he is done.



Session Three

On his third call, I again show “Roger” the fake “Western Union” page that tracks my transfer.

I changed the fake pages before his call so it would show him what I wanted him to believe this time.

Note again, that the URL again appears to be a valid Western Union URL.



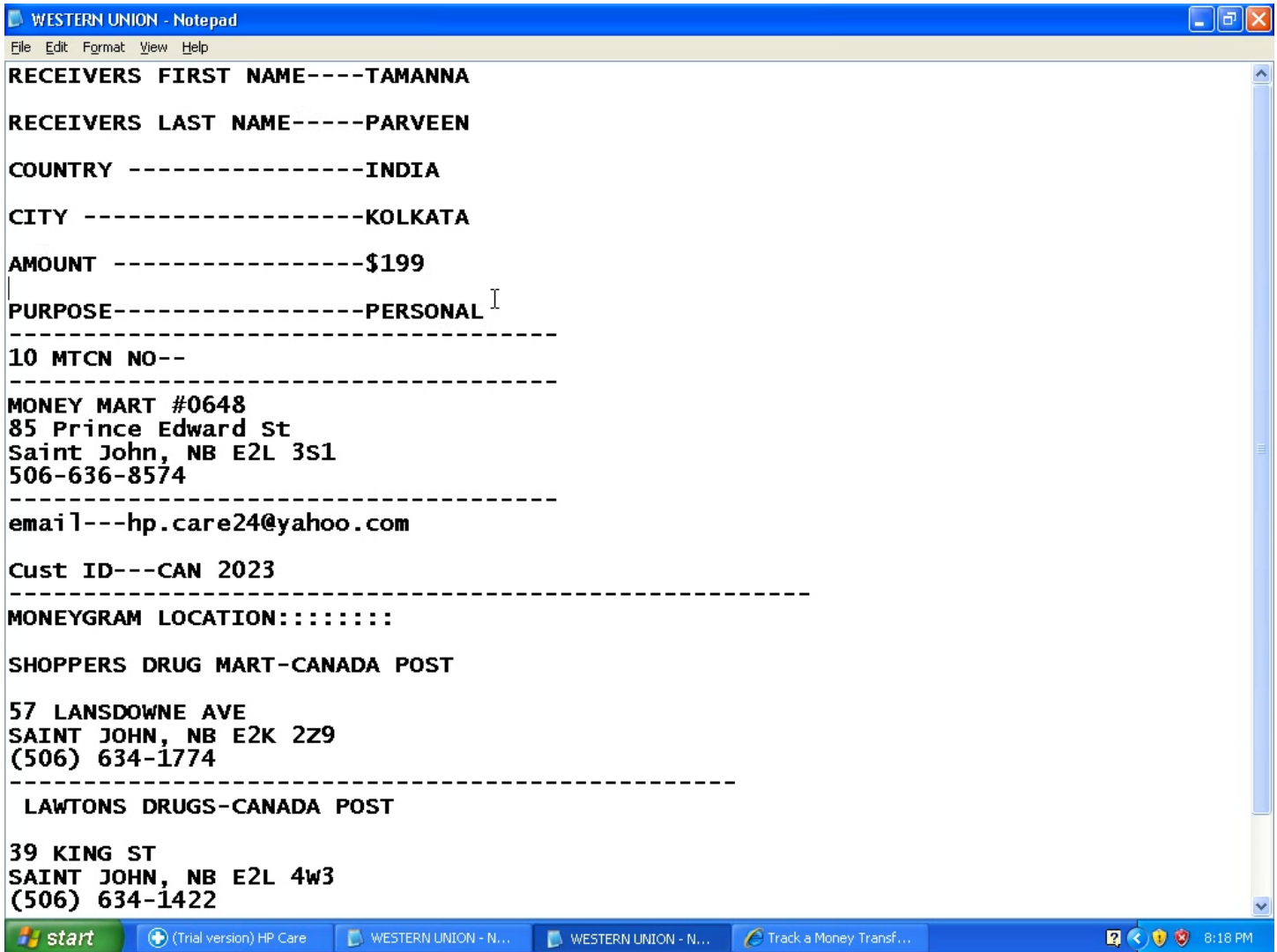
Me: “See, the transfer is working. But the girl said because you are on the old system, and we are on the new system, it will take a week because they have to transfer it manually.”

Me: “Also, the girl at the Western Union office here said that because we have the new system, and India doesn’t, you can’t check the transfer from there. You can only check it from a computer in Canada.”

Roger: “That is too long, let me check with my account manager.”

I think “Roger” was expecting a more instant payment.

Note the fake page verifies the reason for the delay.

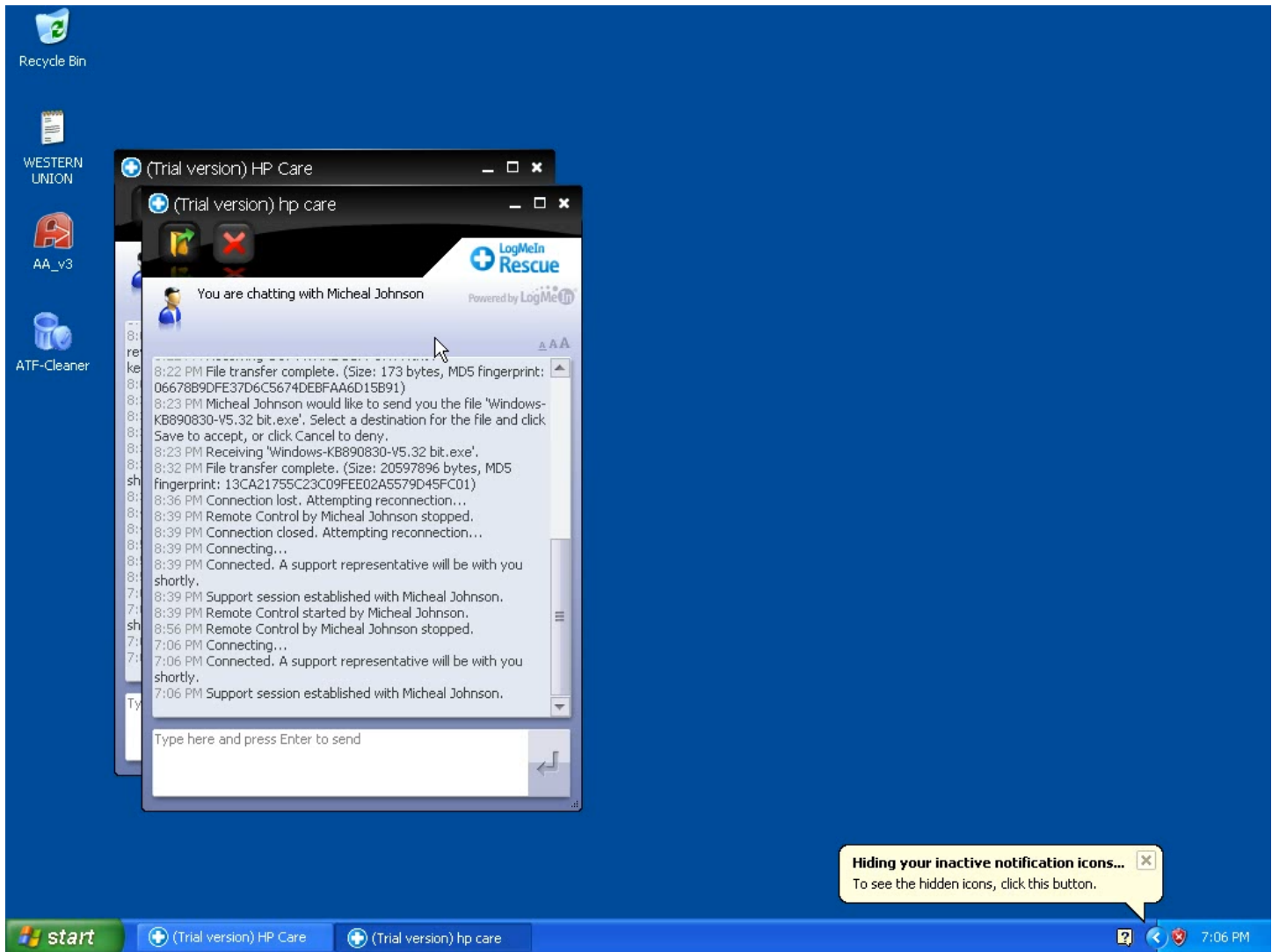


“Roger”, or his “accounts manager” wants the money faster.

Roger: “One week is too long, too long. Tomorrow, you go to the Western Union office, and cancel the transfer. They will give you the money back. Then you go to send a Moneygram instead. You do this tomorrow, ok?”

Of course, I agree and tell “Roger” that I would take care of it in the morning. “Roger” makes me read the addresses to send a Moneygram from the note on my screen.

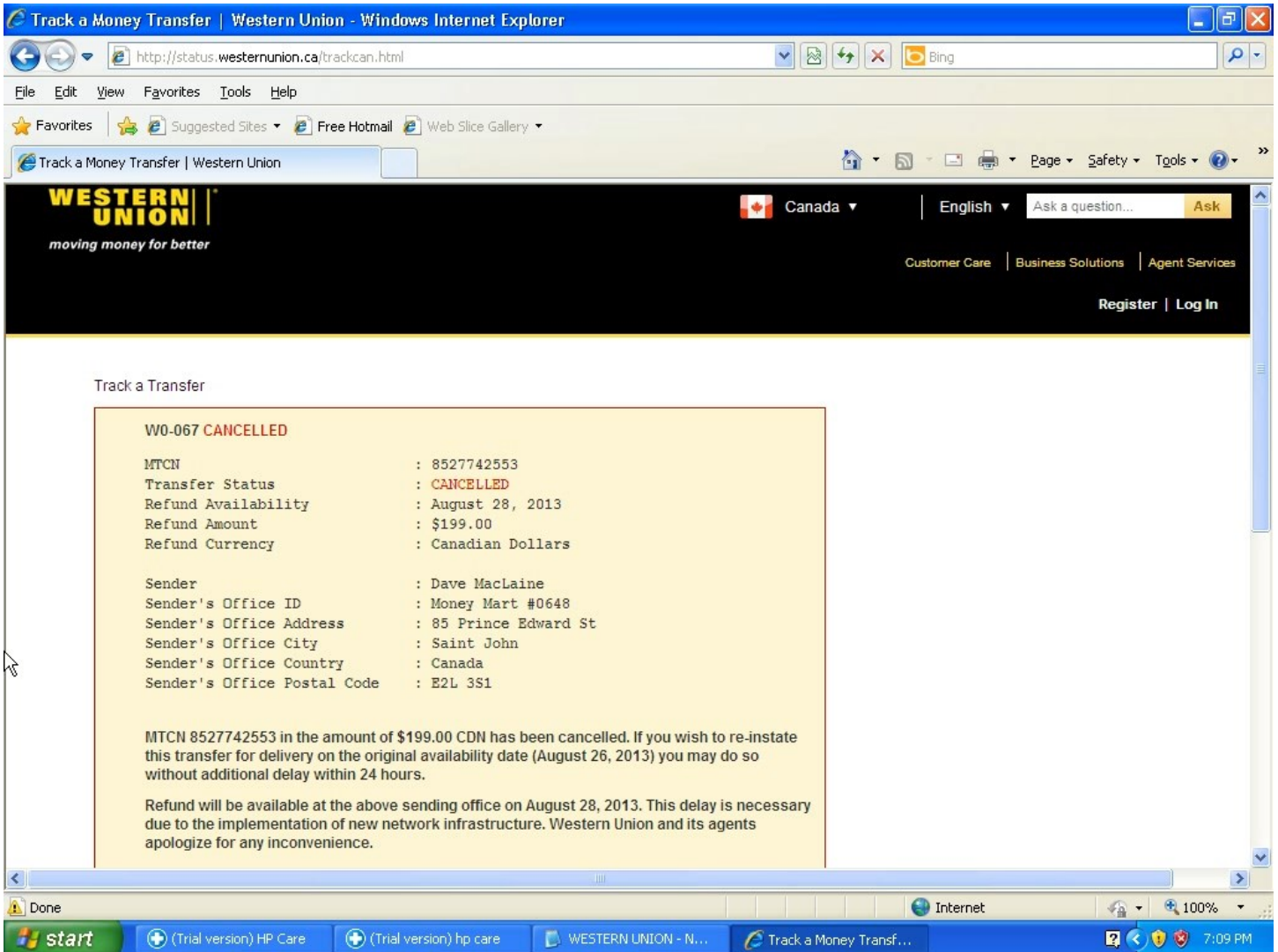
Next, we hang up and “Roger” does all the same things he did on the previous two calls. When he is done, he shuts down the computer.



Session Four

Once again, I allow “Roger” in from remote. Once again, he is using the trial version of the remote access software.

After allowing “Roger” access, he gets additional help via a second remote connection. Apparently, he must think my computer is more than he is able to deal with by himself. Once again, I do my best not to laugh at him.



Track a Money Transfer | Western Union - Windows Internet Explorer

http://status.westernunion.ca/trackcan.html

File Edit View Favorites Tools Help

Track a Money Transfer | Western Union

WESTERN UNION
moving money for better

Canada | English | Ask a question... Ask

Customer Care | Business Solutions | Agent Services

Register | Log In

Track a Transfer

W0-067 CANCELLED

MTCN : 8527742553
 Transfer Status : **CANCELLED**
 Refund Availability : August 28, 2013
 Refund Amount : \$199.00
 Refund Currency : Canadian Dollars

Sender : Dave MacLaine
 Sender's Office ID : Money Mart #0648
 Sender's Office Address : 85 Prince Edward St
 Sender's Office City : Saint John
 Sender's Office Country : Canada
 Sender's Office Postal Code : E2L 3S1

MTCN 8527742553 in the amount of \$199.00 CDN has been cancelled. If you wish to re-instate this transfer for delivery on the original availability date (August 26, 2013) you may do so without additional delay within 24 hours.

Refund will be available at the above sending office on August 28, 2013. This delay is necessary due to the implementation of new network infrastructure. Western Union and its agents apologize for any inconvenience.

start (Trial version) HP Care (Trial version) hp care WESTERN UNION - N... Track a Money Transf... 7:09 PM

Here we go back to my fake “Western Union” page, enter the information, and see that the transfer was indeed cancelled.

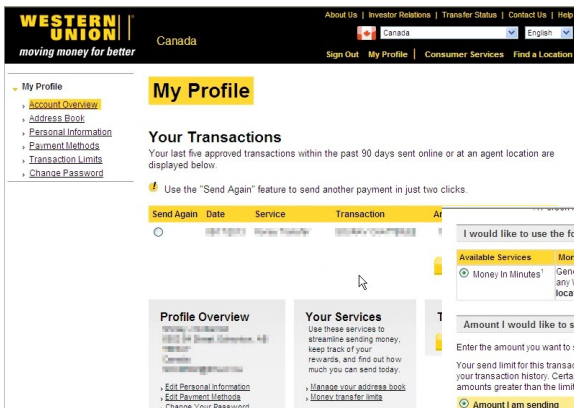
Me: “I cancelled the transfer, but the girl said because the transfer is between the new system and the old system, it will take a week for me to get my money back”.

Roger: “So you didn’t send the Moneygram today?”

Me: “No, Western Union has all my money, I can’t send payment until they give me my money back.”

Roger: “Let me check with my accounts manager...”

I can tell by his voice that “Roger” is starting to get very frustrated. We hang up so I can pretend to go to bed, and “Roger” again works from remote.



WESTERN UNION Canada
moving money for better

Sign Out My Profile Consumer Services Find a Location

My Profile

- Account Overview
- Address Book
- Personal Information
- Payment Methods
- Transaction Limits
- Change Password

Your Transactions
Your last five approved transactions within the past 90 days sent online or at an agent location are displayed below.

Use the "Send Again" feature to send another payment in just two clicks.

Send Again	Date	Service	Transaction	Amount
<input type="radio"/>				

Profile Overview
Send Amount (CAD): 400.00 CA \$
Money Transfer Fees: 20.00 CA \$
Total: 420.00 CA \$

Your Services
Use these services to streamline sending money, keep track of your records, and find out how much you can send today.

- Manage your address book
- Money transfer limits
- Edit Personal Information
- Edit Payment Methods
- Change Your Password

I would like to use the following money transfer service

Available Services	Money is Available	Pay With	What You Need
<input checked="" type="radio"/> Money in Minutes	Generally within minutes at any Western Union Agent location	MasterCard® or Visa® (bank-issued cards only)	The country where money will be received.

Amount I would like to send *

Enter the amount you want to send or to be received.

Your send limit for this transaction is: CA \$ 801.99. Your daily transaction limit will vary based on your transaction history. Certain countries impose lower transaction limits that prevent you sending amounts greater than the limits mandated by local law.

Amount I am sending: 400 Canadian Dollar = Amount that will be received: 23855.06 Indian Rupee

Your Receiver will pick up approximately: 23855.06 Indian Rupee (INR)
Conversion Rate: 1 Canadian Dollar (\$) = 59.6529429 Indian Rupee (INR)

I am sending money to

Your Receiver can pick up your money transfer at any of our Agent Locations in India. Please type the Receiver's name as it appears on the identification they will be presenting to pick up these funds.

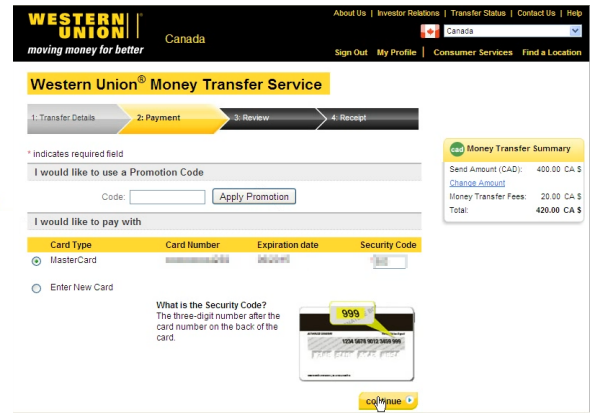
Receiver's First Name: *
Receiver's Last Name: *

Add this person to address book.

Money Transfer Summary

Send Amount (CAD): 400.00 CA \$
Money Transfer Fees: 20.00 CA \$
Total: 420.00 CA \$

Western Union strictly prohibits the use of its internet service to directly or indirectly fund illegal internet gambling and/or illegal activities.



WESTERN UNION Canada
moving money for better

Sign Out My Profile Consumer Services Find a Location

Western Union® Money Transfer Service

1: Transfer Details 2: Payment 3: Review 4: Receipt

Money Transfer Summary

Send Amount (CAD): 400.00 CA \$
Change Amount
Money Transfer Fees: 20.00 CA \$
Total: 420.00 CA \$

I would like to use a Promotion Code

Code:

I would like to pay with

Card Type	Card Number	Expiration date	Security Code
<input checked="" type="radio"/> MasterCard			
<input type="radio"/> Enter New Card			

What is the Security Code?
The three-digit number after the card number on the back of the card.

Thinking I am not watching, “Roger” uses my browser to go to the real Western Union site. He starts to transfer money from a Mastercard belonging to someone in Alberta to someone in India.

It looks like they either recorded this information from a computer they installed spy software on when they were scamming them, or recorded it from their “payment site”. Then they create a Western Union account in the victim’s name, and without the victim’s knowledge, so they can steal more money from them.

Just before “Roger” clicked on Continue to complete the transfer, I killed the power on the Virtual Machine. “Roger” called right away, and I told him we were having a thunder storm and the power went out. He agreed to call next day once the power returned.

I immediately took screen shots (including the name and address of the intended victim) to the city police, and asked them to contact the police in Alberta right away and inform the victim that their charge card was compromised.

Windows XP Professional Setup

Welcome to Setup.

This portion of the Setup program prepares Microsoft(R)
Windows(R) XP to run on your computer.

- To set up Windows XP now, press ENTER.
- To repair a Windows XP installation using Recovery Console, press R.
- To quit Setup without installing Windows XP, press F3.

ENTER=Continue R=Repair F3=Quit

Session Five

For our next session, I tell “Roger” my computer won’t boot.

Me: “It says it wants SYSTEM DISC, I don’t have a system disk. Did my computer break when the power went out last night?”

Roger: “Yes, your Windows is broken because of when the power went out. You need to go to where you got the computer and get two disks, a system disk and a driver disk. Then I will help you fix it.”

I agree, and next day, “Roger” (with much help from his superiors) walks me through getting the computer to boot from the CD. This wasn’t easy and took quite a while.

Me, trying really hard not to laugh: “I don’t understand all this technical stuff”.

While Windows is installing on my computer, “Roger” asks me a bunch of questions, things like where I work and other personal questions, all of which I answer not quite truthfully.

Because I am “one of his best customers” (after all, he seems to be spending most of his scammer career working on my computer), he is going to talk to his manager for me.

They are opening a new office, and need someone for “an exciting work at home opportunity”. All I will need to do is collect payments, and receive my commission. Because I am such a good customer (even though he hasn’t gotten a single penny from me yet), he will recommend my name to his manager. His manager will then call me directly to discuss my possible employment.

I haven’t received a call from the manager yet, but I am pretty sure that when he does call, I will get the job, but there will be a “small fee to secure the position”. That is how this type of scam usually works.

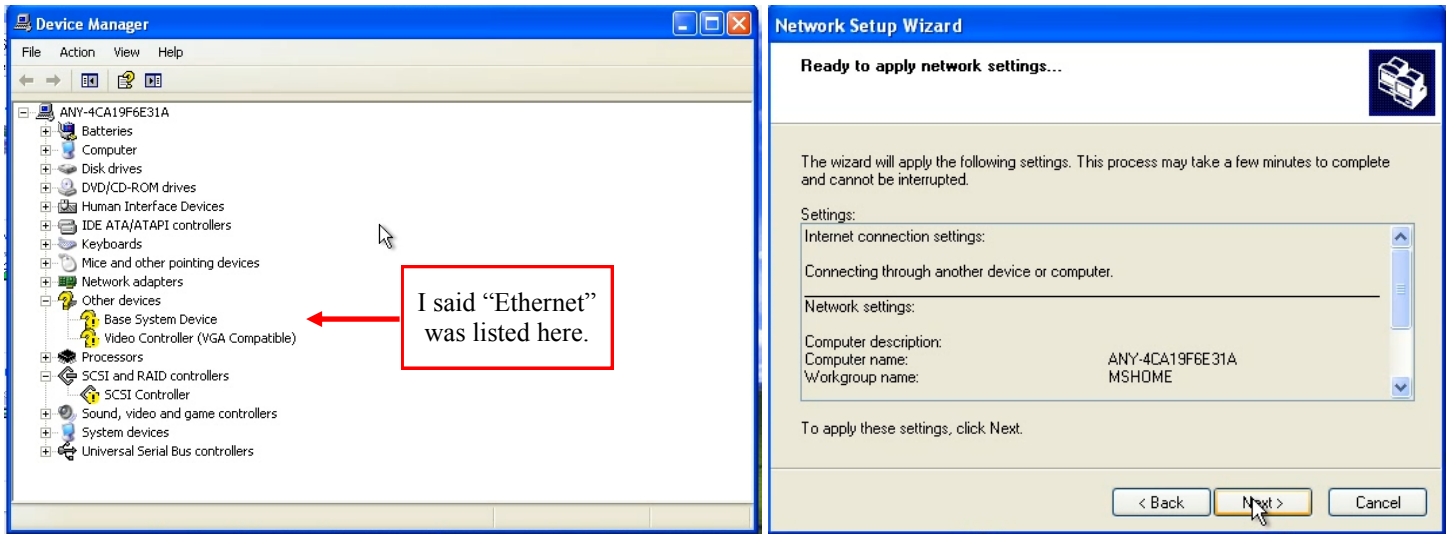
As Windows installs, every so often it requires input. Each time, “Roger” consults with his senior technician and then tells me what to do. Sometimes it takes me longer to accomplish what “Roger” asks, because (as I again tell him) “I don’t understand all this technical stuff”, and “I don’t type very fast”.

“Roger” continues to ask questions and chat.

Me: “Since we formatted my computer and are putting Windows back on, does this mean that all the viruses are gone now?”

Roger: “No no, the viruses hide in a secret place on the computer. I still need to fix it for you.”

This time I cover the mouthpiece because I can’t contain my laughter any longer.



Now Windows is installed, but I tell “Roger” cannot get on the Internet. If I can’t get on the Internet, “Roger” can’t access my computer from remote.

“Roger” consults with his senior technician.

Roger: “You need to put in the drivers disk.”

Me: “I only have one disk, the computer shop didn’t give me any other disk.”

Roger: “I told you to get TWO disks, not only ONE disk, you need the DRIVERS disk, TWO disks not one”.

Me: “They only gave me one disk, and they didn’t have another one.”

This is another one of those times when I need to cover the mouthpiece on the phone so “Roger” can’t hear me laughing.

“Roger” tries to get my Internet connection working. He gets me to open Device Manager and read anything with red or yellow next to it. I lied to him, and read “System Device, Video, and Ethernet” (the Ethernet driver was fine).

“Roger” then gets me to run the Internet connection wizard, and the network setup wizard. I wanted to yell at him “you stupid scammer, nothing you tell me to do is going to work without the Ethernet driver”, but I held my tongue.

We gave up for the night, and I promised to get drivers the disk.

Between Sessions Five and Six

“Roger” called back asking if I got the drivers disc. I told him that even though I bought the computer used, I had it for less than thirty days, so it was still under warranty. I told him I would take it to the computer shop tomorrow, and they would put the drivers in for no charge.

Then “Roger” wanted to know if I sent the MoneyGram.

My wife had a good idea.

Me: “The girl at Moneygram said because of new anti-terrorist regulations in Canada, they need more information to send money out of Canada. They need the name and address of the accounts manager. The information has to come from a government issued ID card, and your accounts manager will need to show the card when he receives the money. If there are any mistakes, he won’t be able to receive the payment.”

Roger: “Let me check with my accounts manager..... Ok, I will give you the information from our other accounts manager from his ID card.”

The name he gave matched the email address that he used to send the spy logs to, so the name and address I got from him is probably real. If it isn’t his, it is for one of his accomplices.

I promised to send the MoneyGram after the long weekend, and he will call me back once the holiday is over.

“Roger” calls back on Tuesday as promised.

Roger: “How are you today? Did you have a good weekend? Did you get your computer back? Did you send the Moneygram?”

Me: “Yes, I got the computer back, they said it is all fixed, but I haven’t hooked it up yet. I went to the Moneygram place, and they mailed you the payment.”

Roger: “Did you get a reference number?”

Me: “No, they mailed it to the address you gave me, they said you don’t need a reference number because they mailed it.”

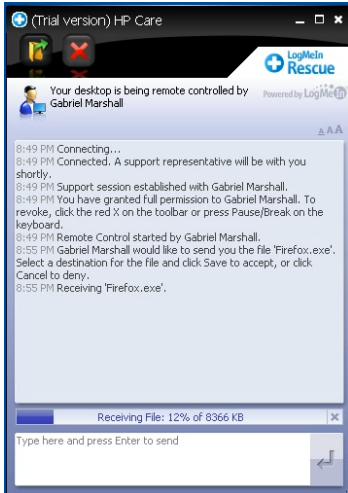
Roger: “How long did they say it would take to get here?”

Me: “I’m not sure, a week or two because it is overseas?”

Roger (sounding disappointed): “Oh, ok.”

I told “Roger” that I had to rush back to work, and I had to work tomorrow night, so he should call me Thursday.

Session Six



“Roger” called tonight. The last few nights I didn’t answer (I had other things to do) but I decided if I wanted to keep him on the hook, I better take his call tonight.

Roger: “We have been worried about you, we have not been able to call you for several days.”

Me: “Oh, at the Giant Tiger where I work, they are renovating the store, so I have to work many nights.”

Roger: “Oh, ok.”

Last time we re-installed Windows from scratch, so “Roger” has to start over from the beginning tonight. He is still using a trial version of the remote access software, but now the name on the software is different. I am guessing that the previous trial has expired.

“Roger” asks me if I use the computer for online banking, because “under California law, I have to secure computers if they are used for online banking.”

“Roger” is also very concerned about payment for “the service”.

Roger: “What about payment, do you have the reference number for the money transfer? It has been forty seven days since we started the service, forty seven days.”

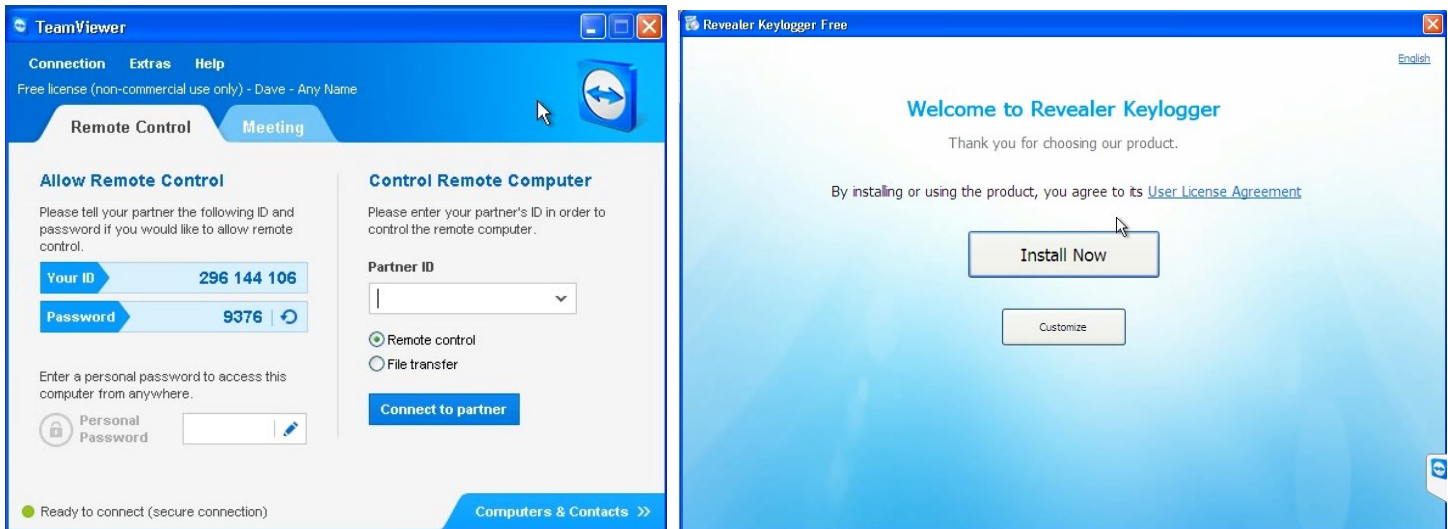
Me: “No, there is no reference number, it was mailed.”

Roger: “What exactly was mailed? Can you tell me exactly what was mailed? When will payment get here? Where did you send it?”

Me: “It was a Moneygram Money Order. It was mailed to the address you gave me, the girl said it will take one or two weeks, depending on the mail in India.”

Roger: ” Ok, ok, my bosses have been asking me about the payment, and I am worried they might fire me.”

I try not to laugh too loudly while “Roger” begins work by installing Firefox.



Now “Roger” installs Team Viewer. It seems that every time he works on my computer, he needs two remote connections. I’m guessing he is just the “voice” while someone else actually accesses the computer.

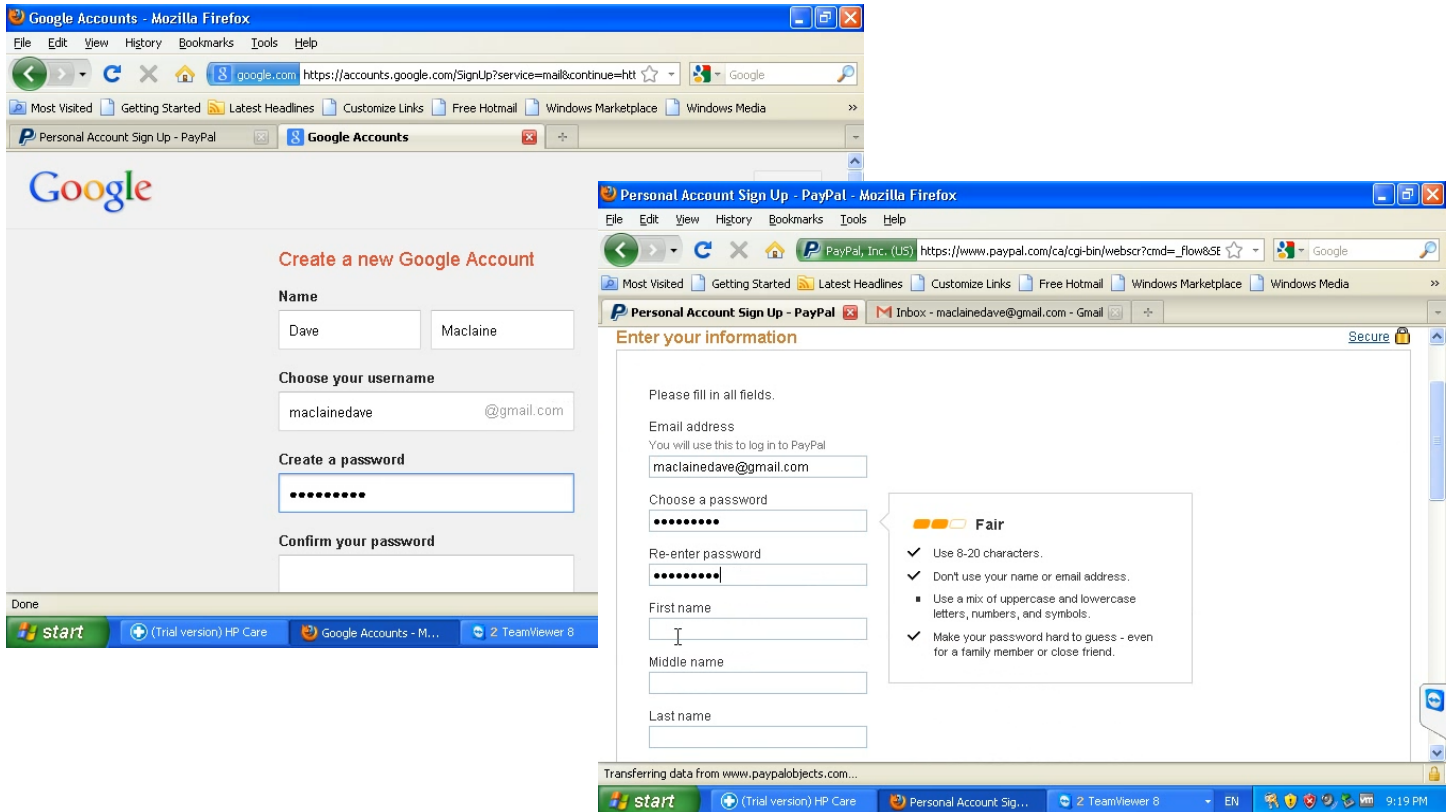
Once again, “Roger” installs a key logging program on my computer. He doesn’t say anything about this, he distracts me by talking about other things.

I play a loud wave file of a clap of thunder into the phone, and tell “Roger” we get thunderstorms all summer. I wanted an excuse in case I had to cut him off suddenly, if he tries to transfer money from someone else to India again.

“Roger” remembers that I don’t have a PayPal account, so he is going to help me create one. But he has other things to talk about first.

He did “recommend my name” for the position with his company. All I have to do is receive payments on his company’s behalf, deposit the cheques, and forward the money, minus my generous commission.

This is another scam. The cheques they send you look real, and when you deposit them, they go into your bank account. You send most of the money back to “Roger.” The cheques take a long time to clear and two weeks later, the cheques bounce. The bank takes the money for the bad cheques out of your account, and you are that much poorer, while the scammer is that much richer.



Now it is time to set up my PayPal account.

Roger: “Ok, so what is your email address”

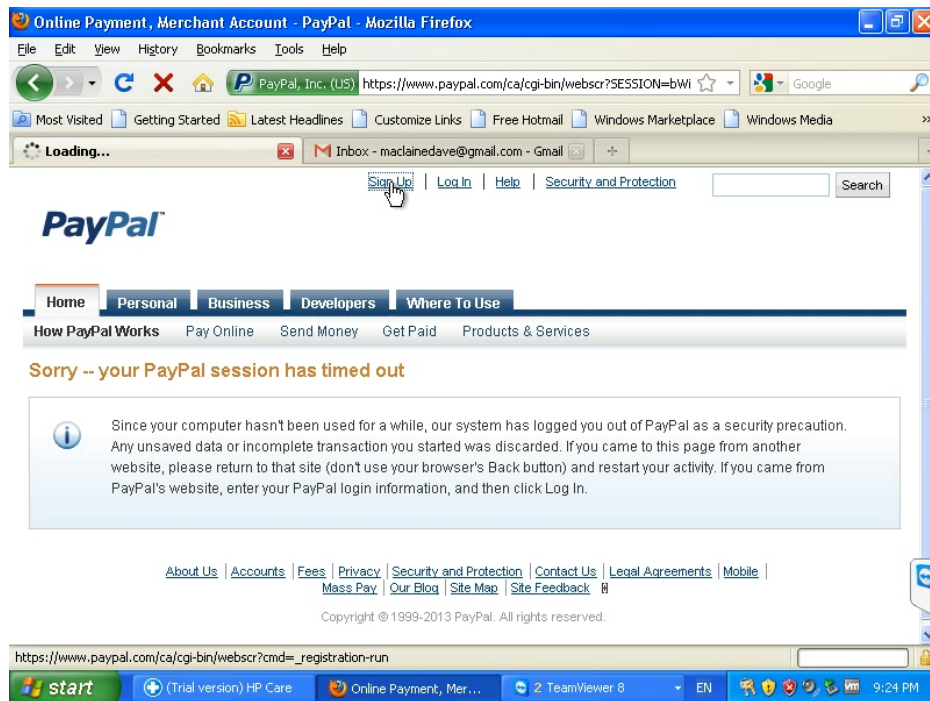
Me: “My wife does all that, she made me an email address, but I never used it.”

Roger: “Ok, we can make you a new email account.”

“Roger” takes me to the gmail page and we create a new gmail account. He gets me to type in a password, and write it down, and tells me not to tell anyone. He doesn’t ask me what it is, why should he? He already installed a key logger.

Then we create my PayPal account, using my new email address. Again, “Roger” gets me to type a secret password, while the key logger is still running silently in the background.

“Roger” tells me to enter my Social Insurance Number and cell phone numbers in the appropriate (but optional) boxes, I told him I didn’t have a cell phone and I don’t know my SIN.



I take my time as we fill out the form, and it takes long enough that it times out.

Roger: “It took too long, it is a secure site, the security times out.”

Me: “Oh, I’m sorry, I don’t type very fast.”

Roger: “We will try again, this time you type in your password, and I will type everything else for you.”

When it comes time to enter the banking info, I don’t know what it is. “Roger” sounds disappointed.

Roger: “You don’t know your bank account type or account number? You don’t have your passbook or statement?”

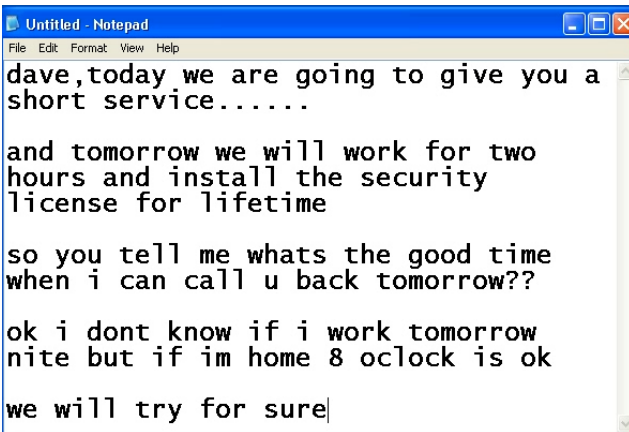
Me: “No, my wife pays all the bills and does all that stuff.”

Roger: “Oh, well when your wife gets home, you get the information and enter it here” (he points the mouse to the banking link on the PayPal screen).

I’m sure that if I did enter any real banking info into a PayPal account that “Roger” created for me (and for which he logged the password), money would quickly disappear from my bank account.

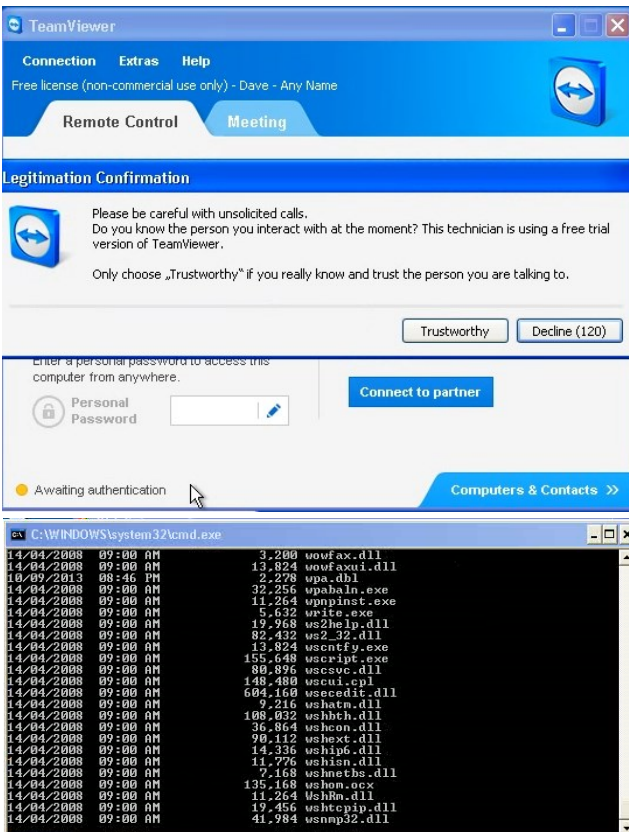


The phone connection isn't very good, "Roger" must be using VoIP from India, and frequently it breaks up. Finally, we can't hear each other at all, and "Roger" types a message for me to hang up and he will call me back.



The new connection isn't much better, so "Roger" types his messages in Notepad. He will "give me a short service" tonight, then tomorrow he will work for two hours and "install the security license for lifetime."

I type to "Roger" that I don't know if I have to work, but he can try at eight. We hang up so "I can go to bed" while "Roger" works from remote.



"Roger" sets Team Viewer so that it will automatically allow him remote access whenever he wants, without needing my permission.

Next he does all the same things he did before we formatted my computer. He did a defrag, ran the disk cleanup, check startup, etc.

Then he downloaded and ran "Software Pro Warranty Phase 1" which, the same as before, does nothing more than endlessly scroll a directory listing in a DOS window. This runs for about an hour, after which "Roger" shuts the computer down for the night.

Session Seven

During previous sessions, “Roger” has had an easy time working on my computer. Everything worked as he expected it to. For tonight’s session, I decided to prepare things ahead of time to make things a bit more challenging for him.

I started by renaming some of the Windows commands. Notepad now opens Paint. Paint opens Calc. And so on. I did the same with some of the system control applets, so when he wants to view the system properties, he will get the accessibility wizard.

Then I added some custom entries to the hosts file, and prepared my firewall. When “Roger” tries to open Google, PayPal, Gmail, and a number of other sites, he gets a random page, a different one with each attempt.

So when “Roger” calls, he logs in from remote and I ask him about the problems the computer is having.

Me: “Oh good, I was waiting for your call, my wife says the computer is infected and all messed up, she can’t get to PayPal or Ebay or Facebook or Banking and a bunch of other places, is it infected?”

Roger: “Yes, because you did not get the daily service it is a problem.”

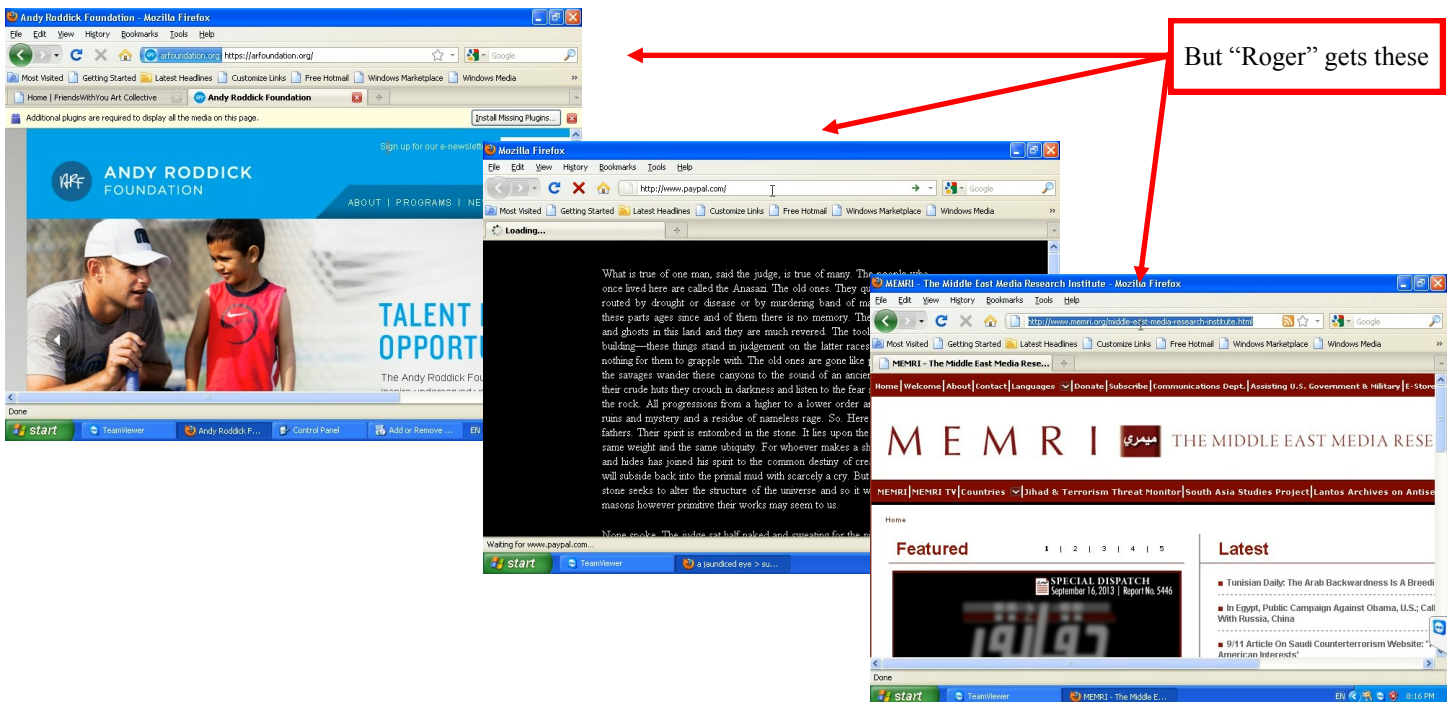
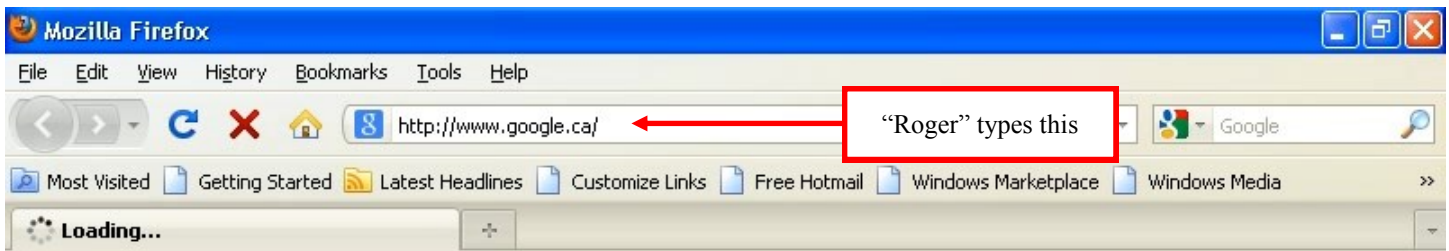
Me: “Ok, but since we have the lifetime service, you will fix it now?”

Roger: “Yes yes, we will fix it.”

But no matter what he does, “Roger” cannot get to a number of pages, the wrong ones keep popping up.

Usually “Roger” sounds confident, but tonight he sounds a little less sure of himself.

We hang up so I can “watch TV” while “Roger” works from remote. But I think watching the virtual machine is going to be more entertaining than watching the TV tonight!

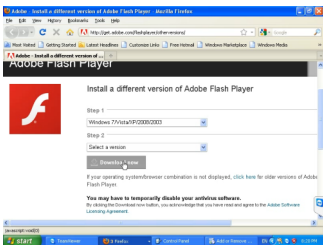


“Roger” thinks I am watching TV while he works, and he will call me later.

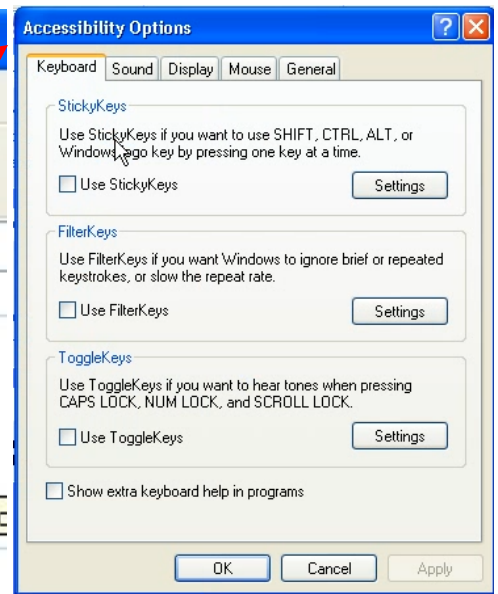
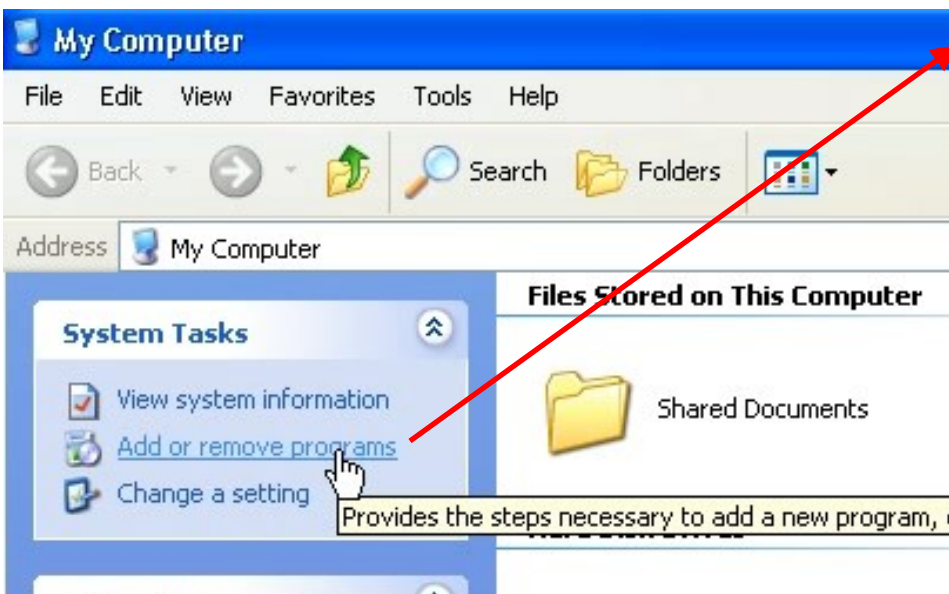
He tries Google a number of times, and Paypal a number of times, and each time, the wrong page pops up. Each time he tries, he gets a different page.

He looks around the system, and does a few things to try to figure out what is happening. Nothing is working right for him.

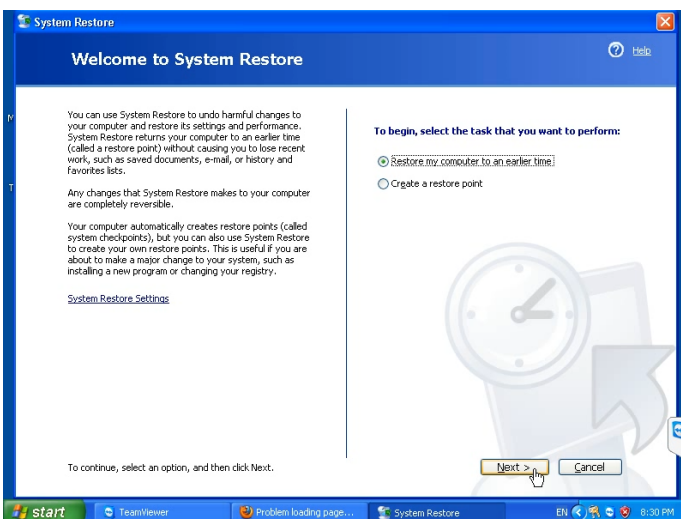
Watching the screen, it is a good thing we hung up because I can't stop laughing. “Roger” has been trying to figure this out for about an hour, and it looks like he is stumped.



Now “Roger” installs the flash player. None of the pages he tried even use flash. I don’t know why he thinks this will help, and, of course, it doesn’t. Installing flash didn’t fix anything at all, and the wrong web pages are still popping up.

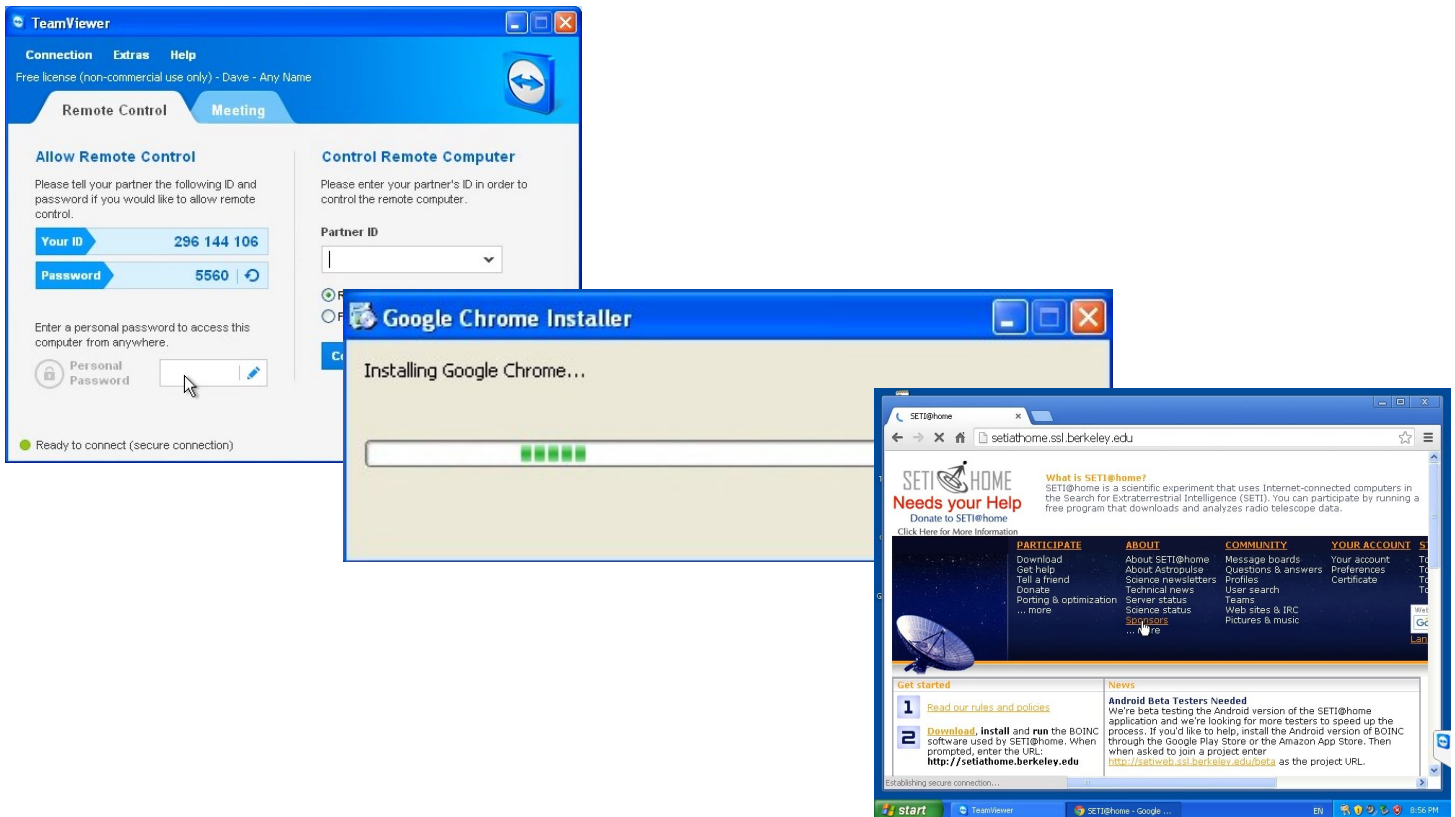


“Roger” discovers that he is having more problems than just the wrong web pages popping up. When he tries to view “Add or remove programs”, instead “Accessibility options” pops up. A number of programs open something different than what “Roger” expects. I burst out laughing, again.



When everything else fails, “Roger” tries the system restore.

The restore runs, setting the system configuration back to a time about a month ago.

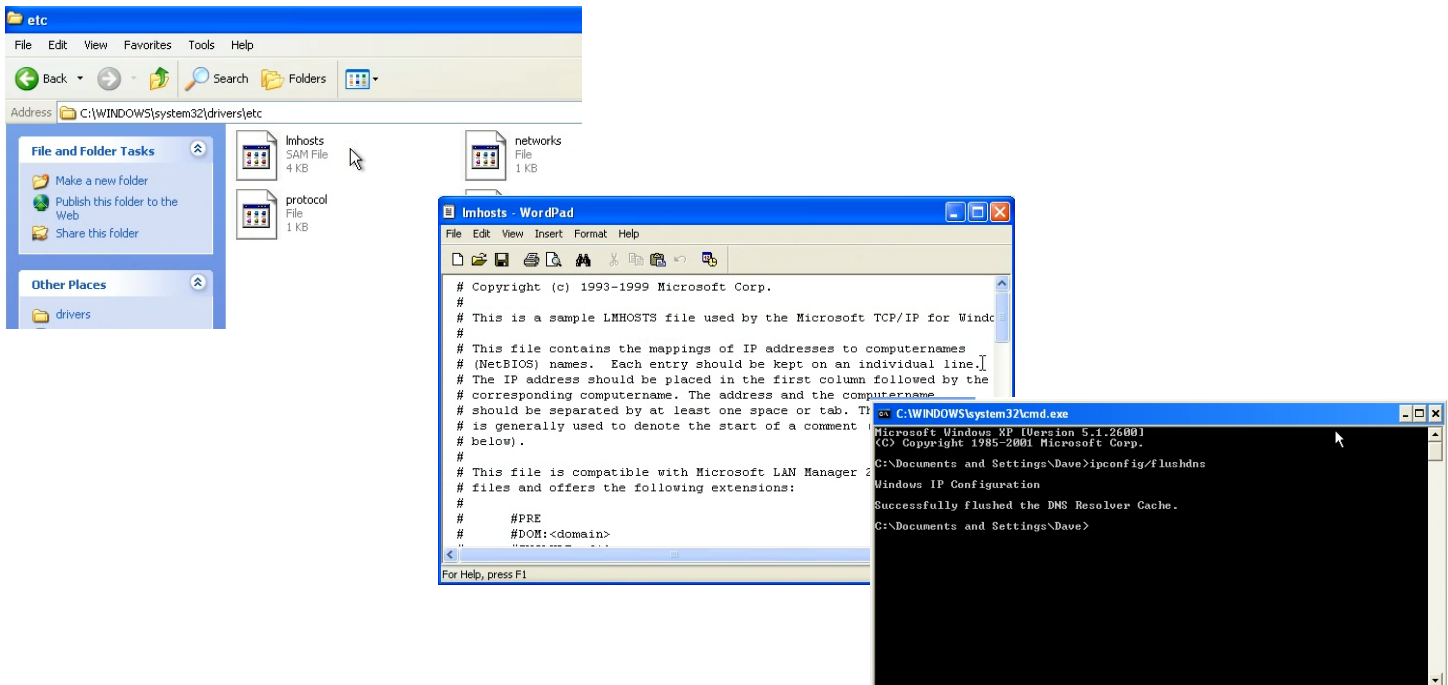


After the system restore, “Roger” calls back and with his help I re-install TeamViewer, and “Roger” logs into my virtual machine. I’m sure he is hoping that the restore has fixed all his problems. Once he is connected, we hang up again while he works.

Now he installs Google Chrome. Last time, he told me never to use anything except Firefox, but I guess Chrome is the browser of the day today.

“Roger” types “www.google.com” in the address bar, but the SetiAtHome page pops up. I guess the system restore didn’t help.

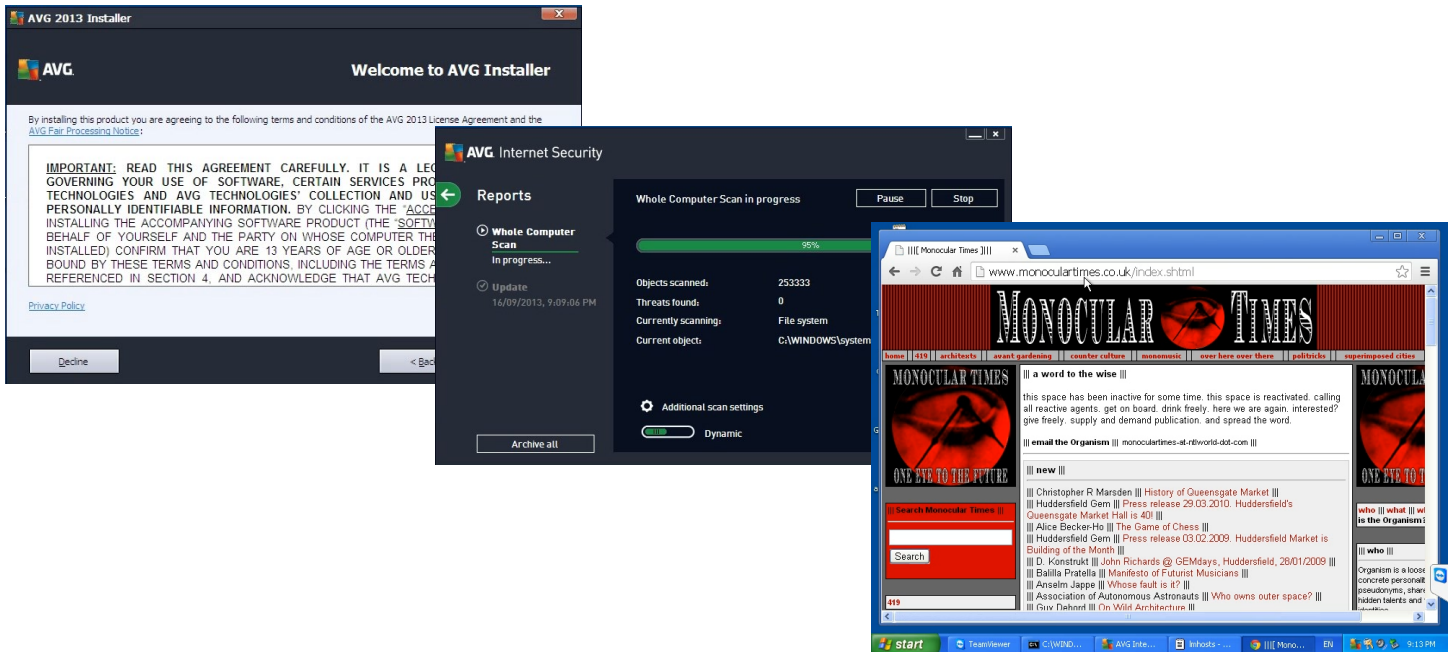
He tries Google a couple more times, and each time he lands on a different page.



This is where it becomes more obvious that “Roger” has help. My guess that the boiler room where he works has one or two slightly more technical people. This person (or persons), who “Roger” regularly consults, is probably responsible for writing the script, and directing the people who actually make the calls, and for handling anything unusual. And by now, my computer must appear unusual to them.

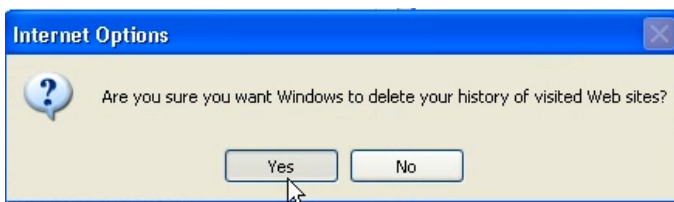
After snooping around the computer, “Roger” goes to the etc directory, and opens the lmhosts file. He is close, he wants the hosts file, not lmhosts, but the hosts file is hidden. “Roger” doesn’t turn on viewing of hidden files, so all he sees is lmhosts. Since this file doesn’t have anything unusual, he closes it and putters around the system some more. He comes back and opens the lmhosts several times, but it is the same each time.

He tries a few things, such as flushing the DNS cache, but nothing helps. Judging by the length of time between things “Roger” tries, I’m guessing he is looking up solutions on Google.



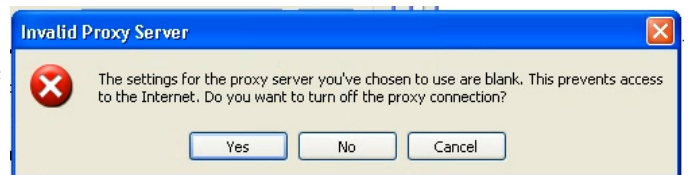
Since nothing he has tried so far has worked, “Roger” transfers the trial version of AVG to my computer and installs it. He runs it but doesn’t find any infections. I didn’t think he would find any viruses, because I didn’t put any in there for him to find.

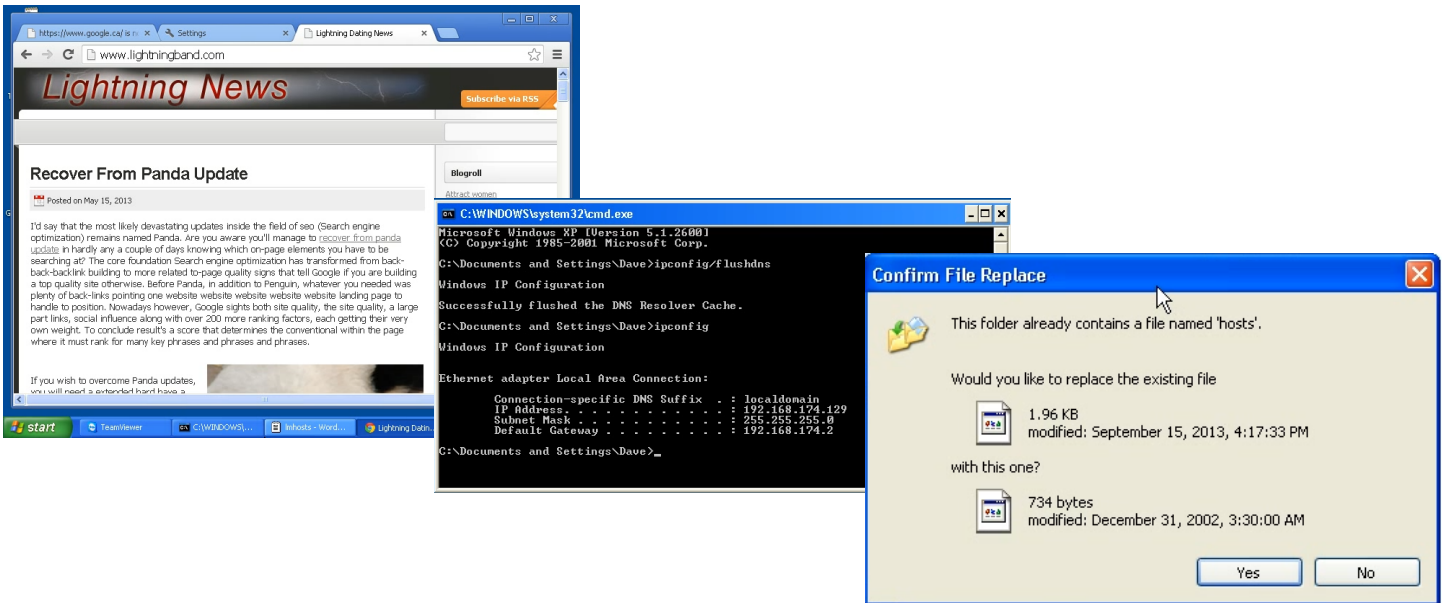
The wrong web pages are still opening every time “Roger” tries to go to Google or many other sites. My wife in the next room hears me burst out laughing.



Now “Roger” tries clearing the Internet Explorer cache and history. I shake my head, wondering why he thinks this should help when he was using Google Chrome.

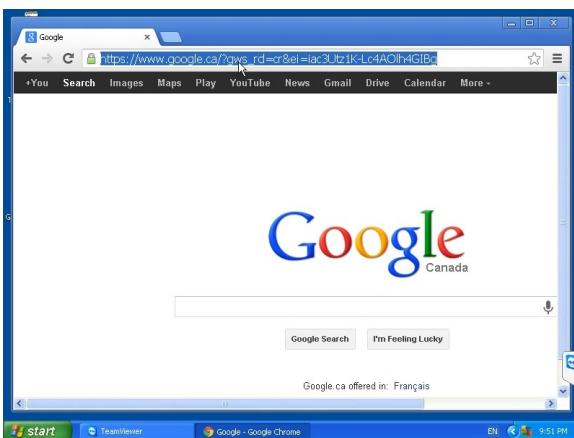
He also deletes the temp files, checks the proxy settings, and does a few other things. “Roger” tries setting Internet Explorer to automatically detect a proxy server, but this doesn’t work. There is no proxy server on my network. Even if there were, I doubt that he would be able to configure Internet Explorer for it, it is obvious at this point the most of “Roger’s” technical skill involves looking for solutions on Google, none of which he fully understands.





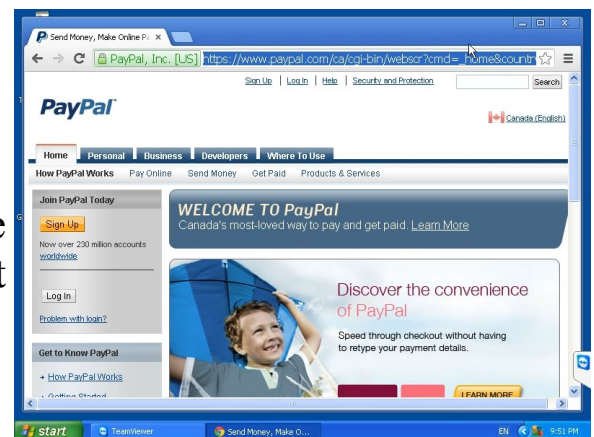
“Roger” tries Google, Bing, and PayPal several more times. Each time a random page pops up. He carefully goes through ALL the settings in the Internet Explorer control panel applet, and resets everything. He then resets all the settings on Chrome, and checks my IP address in a command prompt.

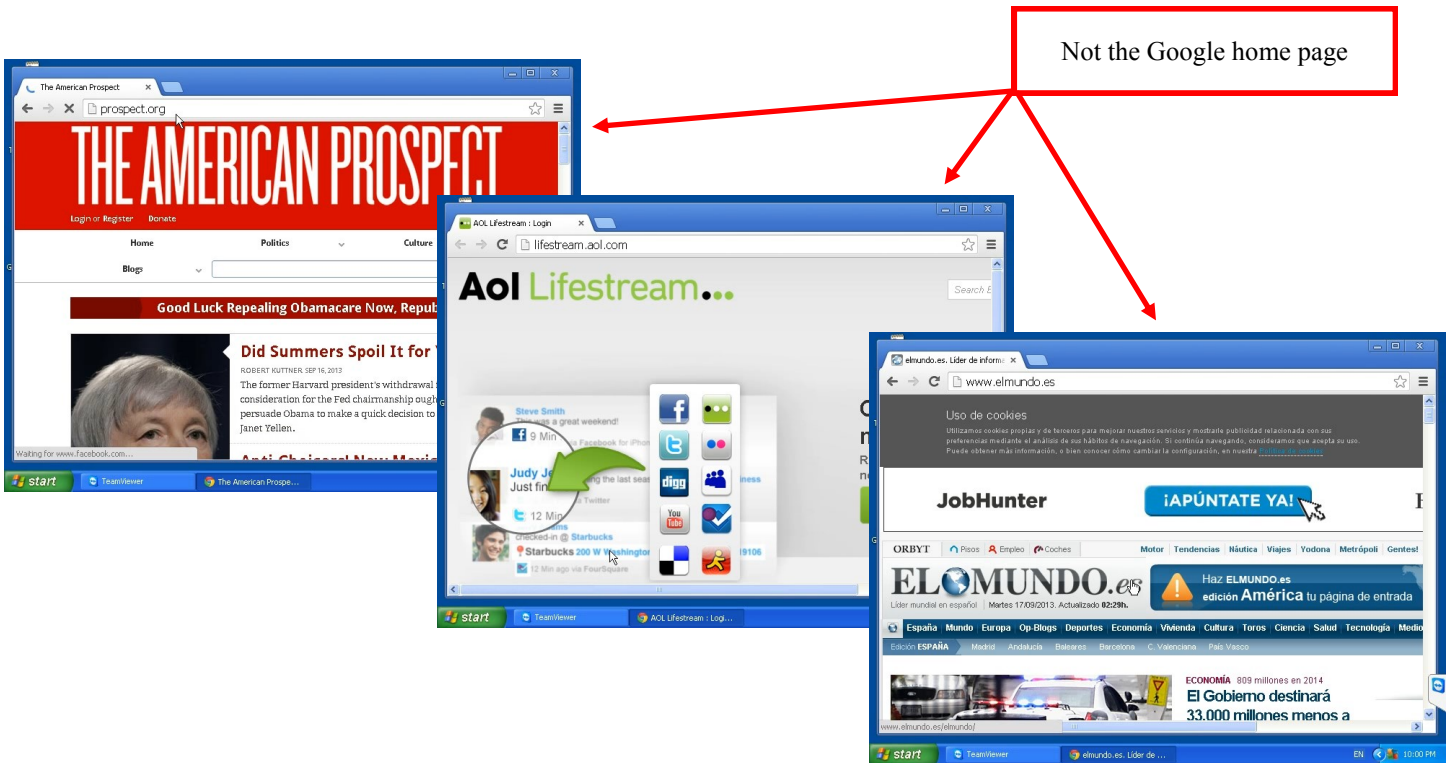
After a long wait, no doubt while he searches more on Google, “Roger” transfers a new hosts file to my computer, and overwrites my custom hidden one.



Success! “Roger” can now get to Google and PayPal. I’m guessing that “Roger” is pretty proud of himself at this point.

He immediately creates a restore point, in hope that he can quickly correct this problem if it occurs again.





After creating the restore point, “Roger” heads back to Google., but the wrong page comes up again! And again!! And again!!!

My sides are getting sore from all the laughing I have been doing during this session.

```

hosts - WordPad
File Edit View Insert Format Help
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
# 102.54.94.97    rhino.acme.com    # source server
# 38.25.63.10    x.acme.com        # x client host

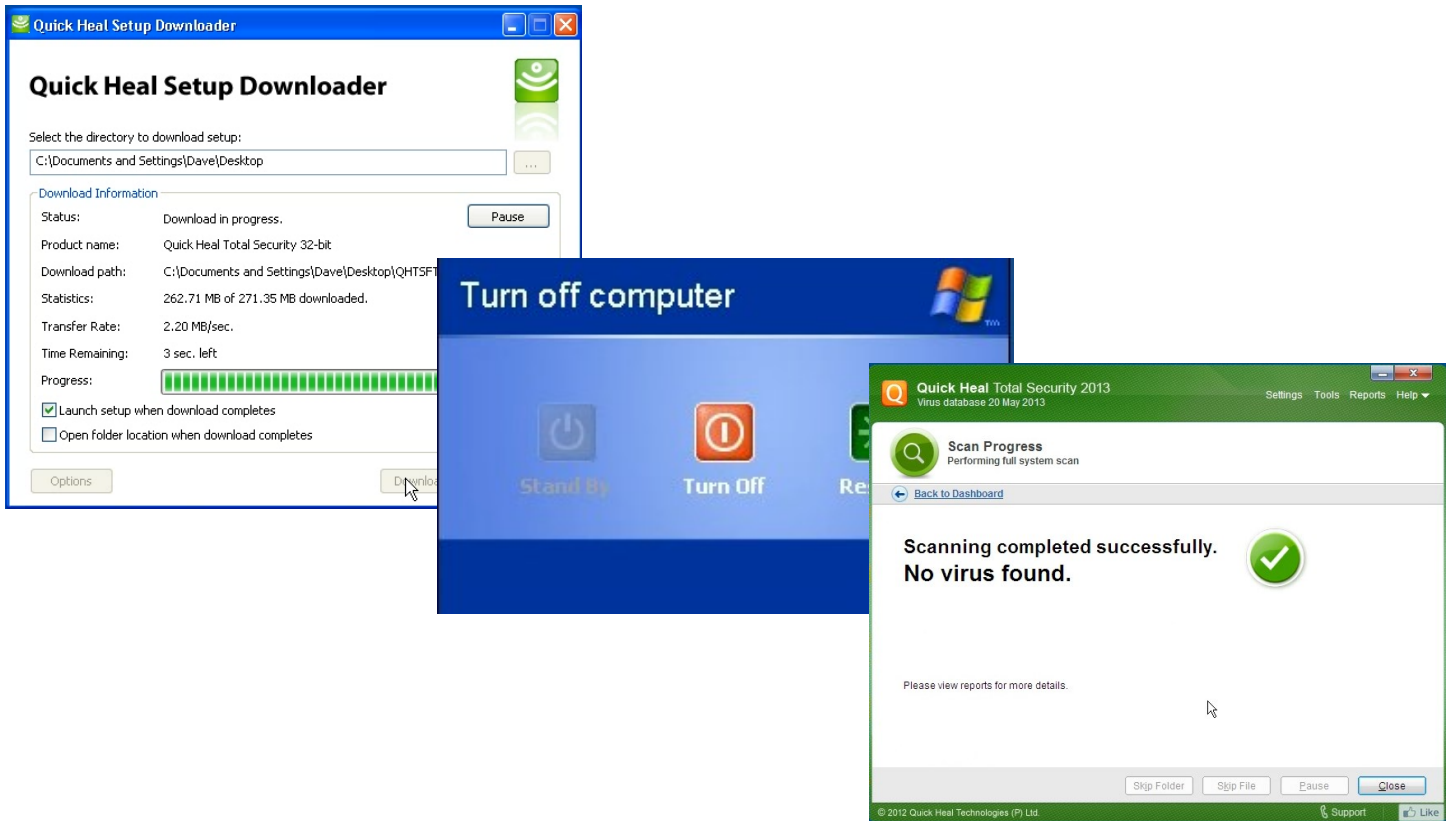
127.0.0.1        localhost

```

“Roger” checks the hosts file he just uploaded, and it is correct, the default Windows one.

The reason things went wonky on him again is because I simply took all the entries I had made in the hosts file, and pasted them into the nameserver on my firewall. Since the cause of the problem now isn’t in the virtual machine, it is unlikely that “Roger” will be able to figure it out.

At this point, I wonder if scammers ever get nervous breakdowns, and if “Roger” is about to have one.



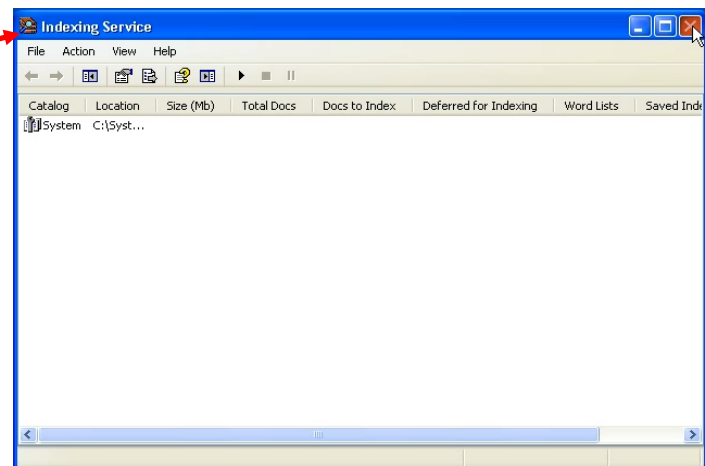
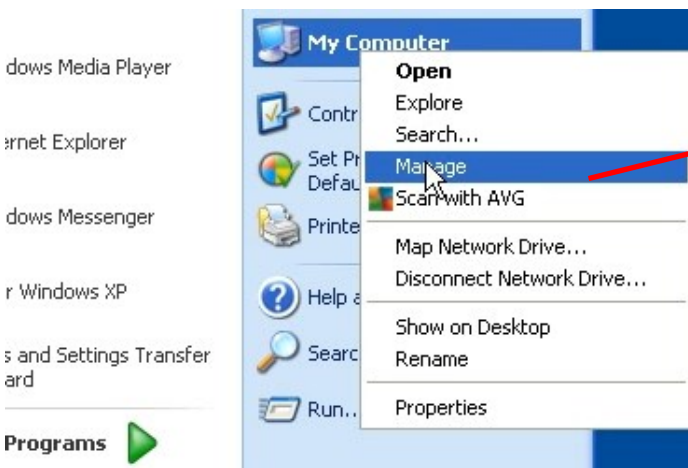
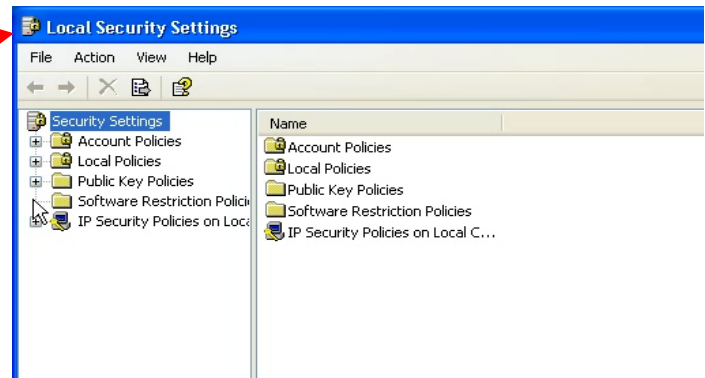
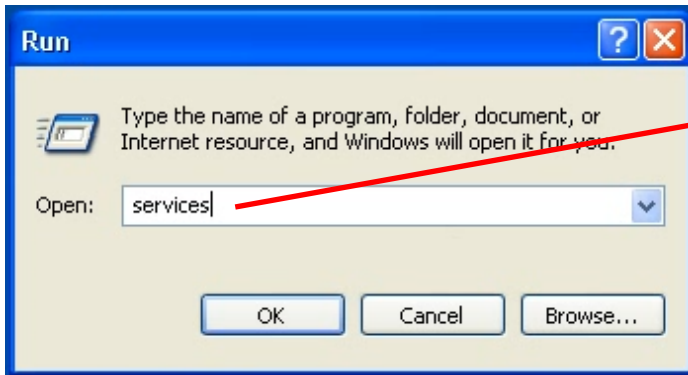
“Roger” now installs Quick Heal. It requires a reboot after installation, so he sets his remote access software to allow unattended remote login, and reboots the computer.

Once the system has rebooted and “Roger” has logged back in, he performs a scan with Quick Heal. Of course, just like the scan with AVG, nothing is found.

I am tempted to install a few viruses just for “Roger’s” benefit, so there will be something for all his scans to find.

“Roger” proceeds to check everything he can think of, many of which could have any bearing on the problem he is having: Windows time settings, Windows firewall, free disk space, automatic updates, and more.

The wrong web pages still pop up when he tries Internet Explorer and Chrome again.



“Roger” also continues to experience other difficulties. When he tries to run the Services management applet, he gets the Local Security settings. When he tries to select Manage from the Computer context menu, he gets the Indexing Service.

I guess this sort of thing can happen if you rename some of the commands and applets before “Roger” calls. By this time, I’m too tired to laugh. “Roger” has been working for over three hours tonight.

After this, nothing happens on the screen for a while, and I want to go to bed, so I kill power to the virtual machine. “Roger” doesn’t call when I do, and he didn’t call the next night either, so I suspect he has had enough.

I wonder if I’ll hear from him again?

A Few Days After Session Seven

I haven't heard from "Roger" for several days, since he couldn't figure out why my computer wouldn't co-operate with him.

Here are a few random facts of interest about "Roger" and his attempted scam:

- A scammer makes a cold call and informs the victim that their computer is infected and needs to be cleaned. The scammer can do this from remote for a fee.
- The scammer works from a script, and sometimes can adlib if necessary, sometimes not.
- The scammer works in a "boiler room" under the direction of one or more scammers who are more technically knowledgeable, but still not real technicians.
- The payment site that they ask you to use may or may not capture your charge card information if you fall for the scam.
- The scammer will install spy software on your computer to gather information that may be used in the future. The information they want would include charge card and bank account numbers and passwords, PayPal login information, and any other information that may be useful to them.
- Once the scammer has banking/charge card/PayPal information, they will use it to steal money using a Western Union money transfer (which is NOT recoverable) or other money transfer service, so if you fall for the scam, you stand a good chance of losing more than just the initial payment.
- The scammer is not a single person who accesses your computer from remote, he is likely just the voice you hear. He will initiate remote access to your computer, and talk to you while he performs some simple tasks (many of which are useless but designed to make you think he is working), and then he will turn the remote connection over to someone else who has a bit more technical skill.
- The scammer runs additional scams, such as the fake cheque scam, that he may try to use on you.

Anyway, that is all for now. If "Roger" calls back, I will post an update.

Over A Week After Session Seven

I guess “Roger” hasn’t given up yet.

The “accounts manager” called from India. Apparently, they still want payment. My wife said to call back at eight in the evening when I am home.

Sure enough, “Roger” calls back at about eight. I tell him I am busy, he will have to call back tomorrow.

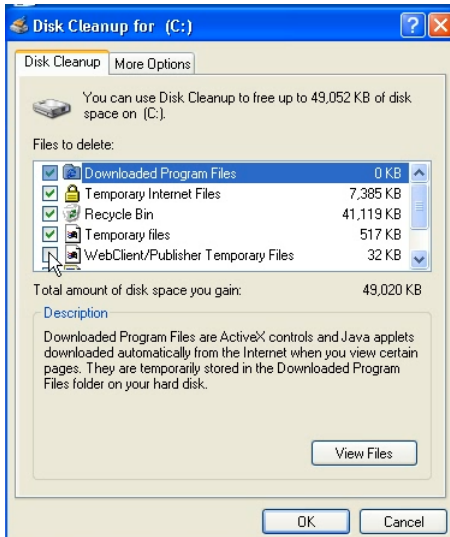
He wants to talk for a moment about the payment, he is getting concerned. I promise to talk to the girl at the money place and have answers for him when he calls tomorrow “to finish the service” on my computer.

He suggests that I should get my money back and this time send it Western Union. I didn’t remind him that I have already tried that (or, at least he thinks I did), and he told me to cancel it because it took too long.

I set things up again with my DNS and web servers to cause a bit of confusion on the virtual machine, so “Roger” should have an interesting time trying to fix things if he calls tonight.

If “Roger” figures it out and tries to manually set a DNS server in the network card properties, it won’t help. My firewall is set to redirect all DNS queries from the virtual machine to my DNS server. No matter what “Roger” puts in for DNS settings, it will still use the DNS server I want.

Session Eight



The first thing “Roger” asked at the beginning of session eight was about the payment.

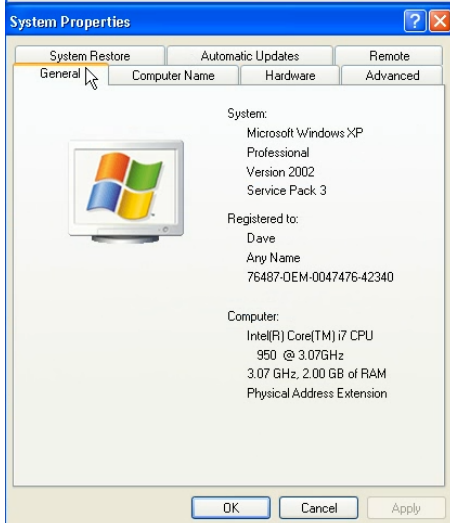
Roger: “My accounts department still has not got the payment. Can you send the payment again?”

Me: “I will ask the girl at the money transfer place about it tomorrow.”

Roger: “I am getting in trouble with my accounts department, they are blaming me for no money.”

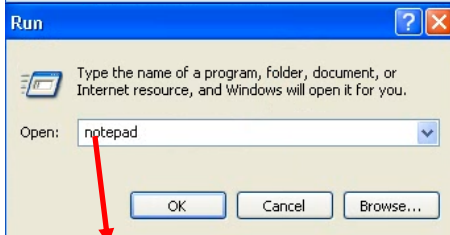
Me: “Ok, I will go to the money transfer place again tomorrow.”

Roger: “Ok ok”.

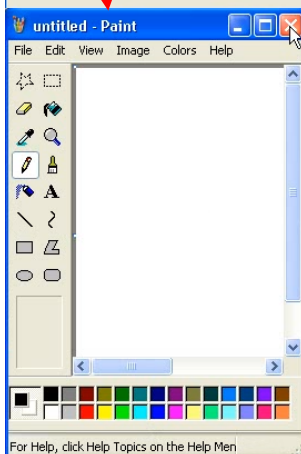


“Roger” logs in from remote, and we hang up while he works. He does some of the same things again he did in the other sessions.

He does a disk cleanup, runs ATF Cleaner, and pokes around the system a bit, looks at settings and things, and in general doesn’t accomplish much.

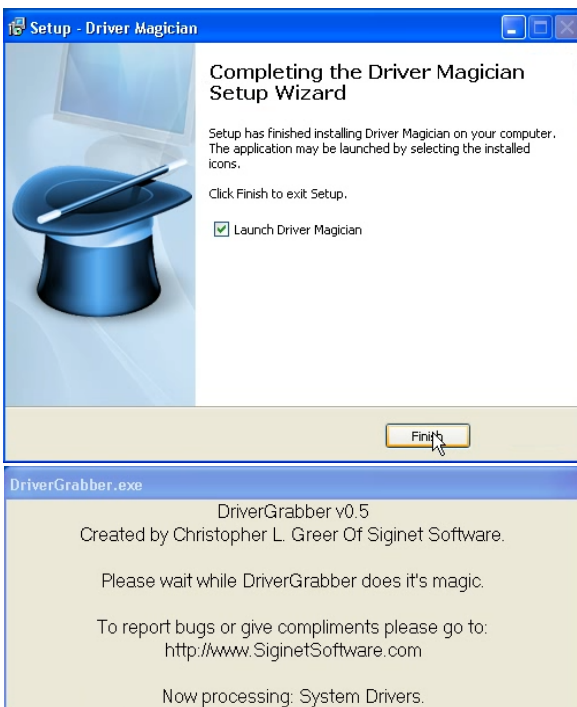
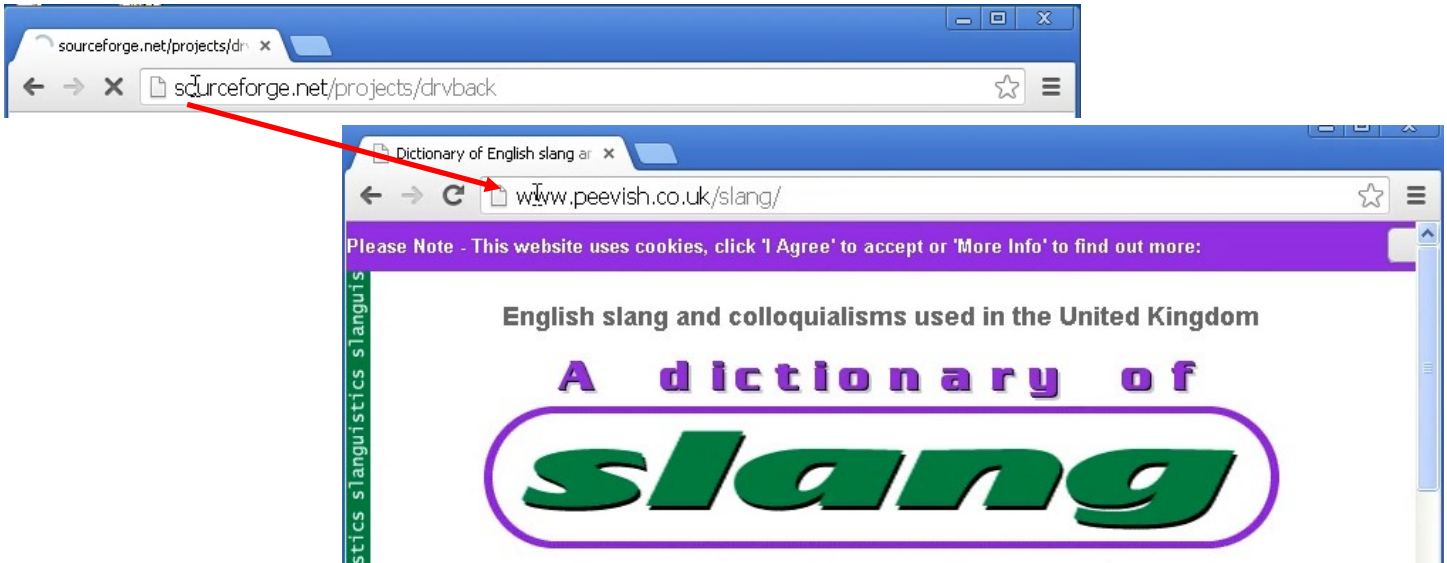


Then he runs “Software Pro Warranty” and the endless directory listing runs for a while.



He tries to open Notepad again, but as before, Paint comes up. Defrag doesn’t work. Other programs don’t work. The wrong things keep opening.

“Roger” isn’t having much luck tonight.



Of course, the web still isn't working properly. My custom DNS and web server setup are still active. Just for fun, whenever "Roger" types in a web address, I quickly add it to my DNS server and redirect it to a random page. I can usually do this pretty quickly, so the page "Roger" wants never comes up.

Now he installs a couple of driver utilities. Since the web isn't working on my virtual machine, he has to download the utilities on his computer, and transfer them to my computer using the remote access software. Of course, running these utilities doesn't help.

Poor "Roger", nothing seems to be working for him, again.

At this point I almost feel sorry for him, but I remember that he is a thief that steals money from innocent people, and more often than not his victim is an elderly person who lacks the knowledge to spot the scam. So I think "Roger" deserves all the frustration I can give him.

After a while, "Roger" gives up for the night and shuts down the computer.

Final Notes

“Roger” left a voicemail last night, he has not been able to reach me. It has been about three months since he first called. I have learned what tactics this type of scammer uses to convince a victim to allow remote access to their computer, I have learned what they do to a victim’s computer once they have access, and I have caused him hours of frustration.

So I am done with “Roger”. If he calls, I will tell him I got the computer fixed elsewhere since we was unable to do so, and hang up on him.

Different groups of scammers may use different techniques and do different things to the victim’s computer, so my virtual machine is ready for when the next scammer calls. But for now, I guess this is

The End