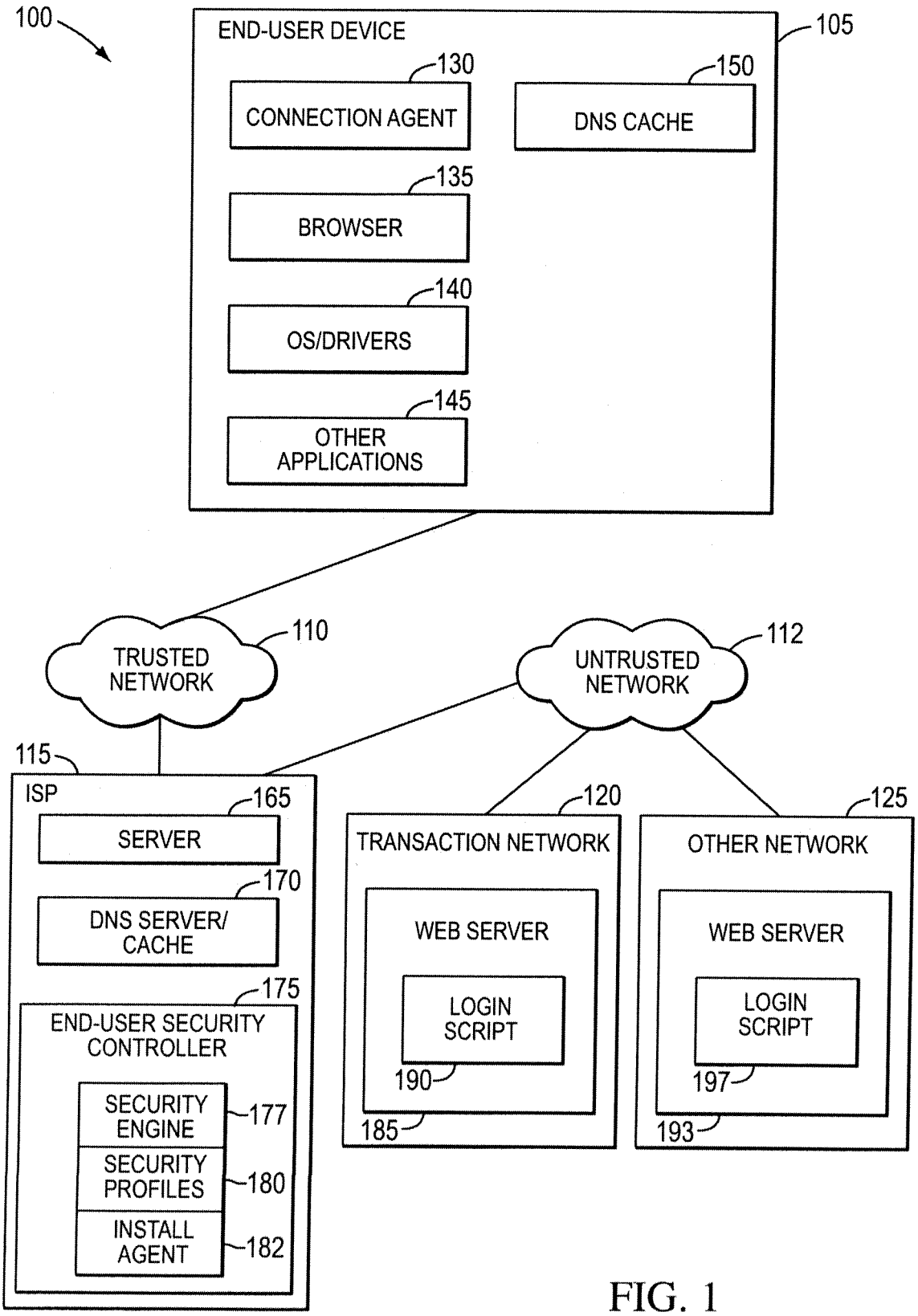

100
END-USER DEVICE
105
130
CONNECTION AGENT
150
DNS CACHE
135
BROWSER
140
OS/DRIVERS
145
OTHER APPLICATIONS
TRUSTED NETWORK
110
UNTRUSTED NETWORK
112
115
ISP
165
SERVER
170
DNS SERVER/ CACHE
175
END-USER SECURITY CONTROLLER
SECURITY ENGINE
177
SECURITY PROFILES
180
INSTALL AGENT
182
TRANSACTION NETWORK
120
WEB SERVER
LOGIN SCRIPT
190
185
OTHER NETWORK
125
WEB SERVER
LOGIN SCRIPT
197
193

FIG. 1

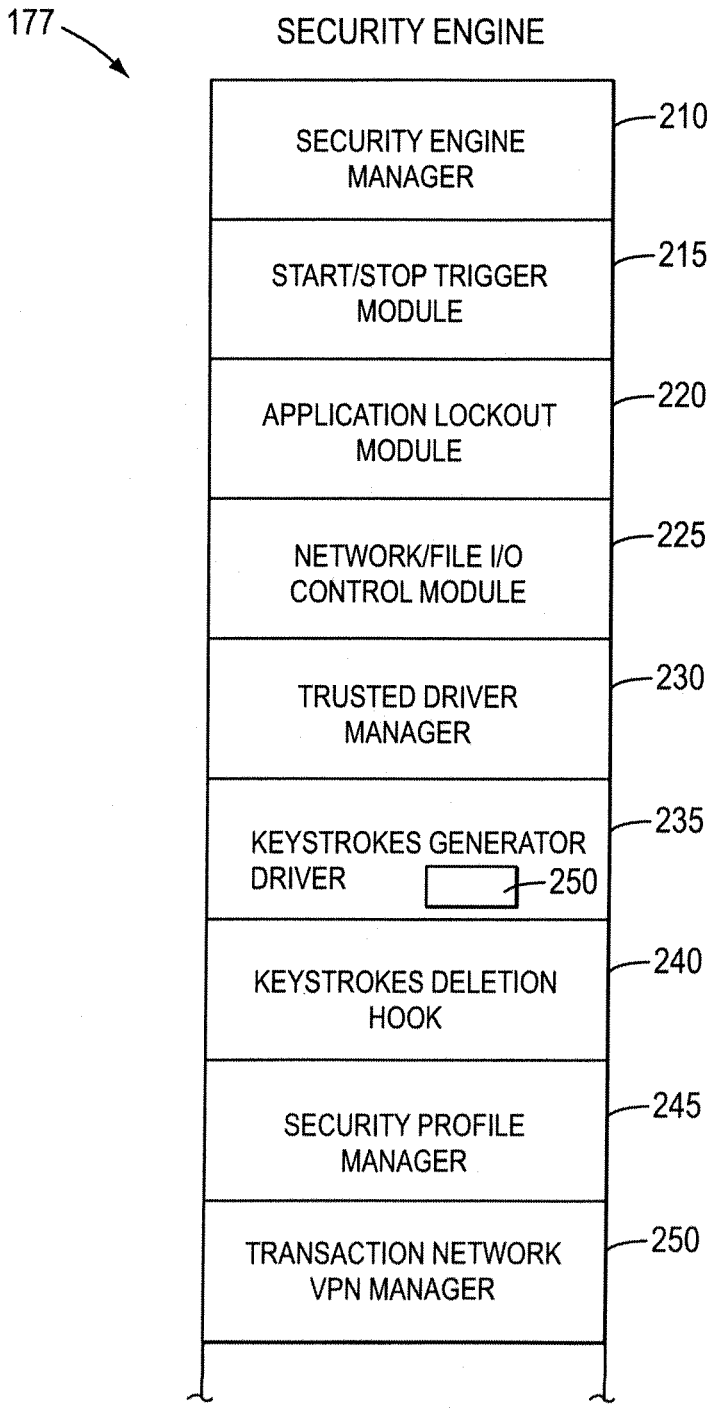

177
SECURITY ENGINE
SECURITY ENGINE MANAGER
210
START/STOP TRIGGER MODULE
215
APPLICATION LOCKOUT MODULE
220
NETWORK/FILE I/O CONTROL MODULE
225
TRUSTED DRIVER MANAGER
230
KEYSTROKES GENERATOR DRIVER
250
235
KEYSTROKES DELETION HOOK
240
SECURITY PROFILE MANAGER
245
TRANSACTION NETWORK VPN MANAGER
250

FIG. 2

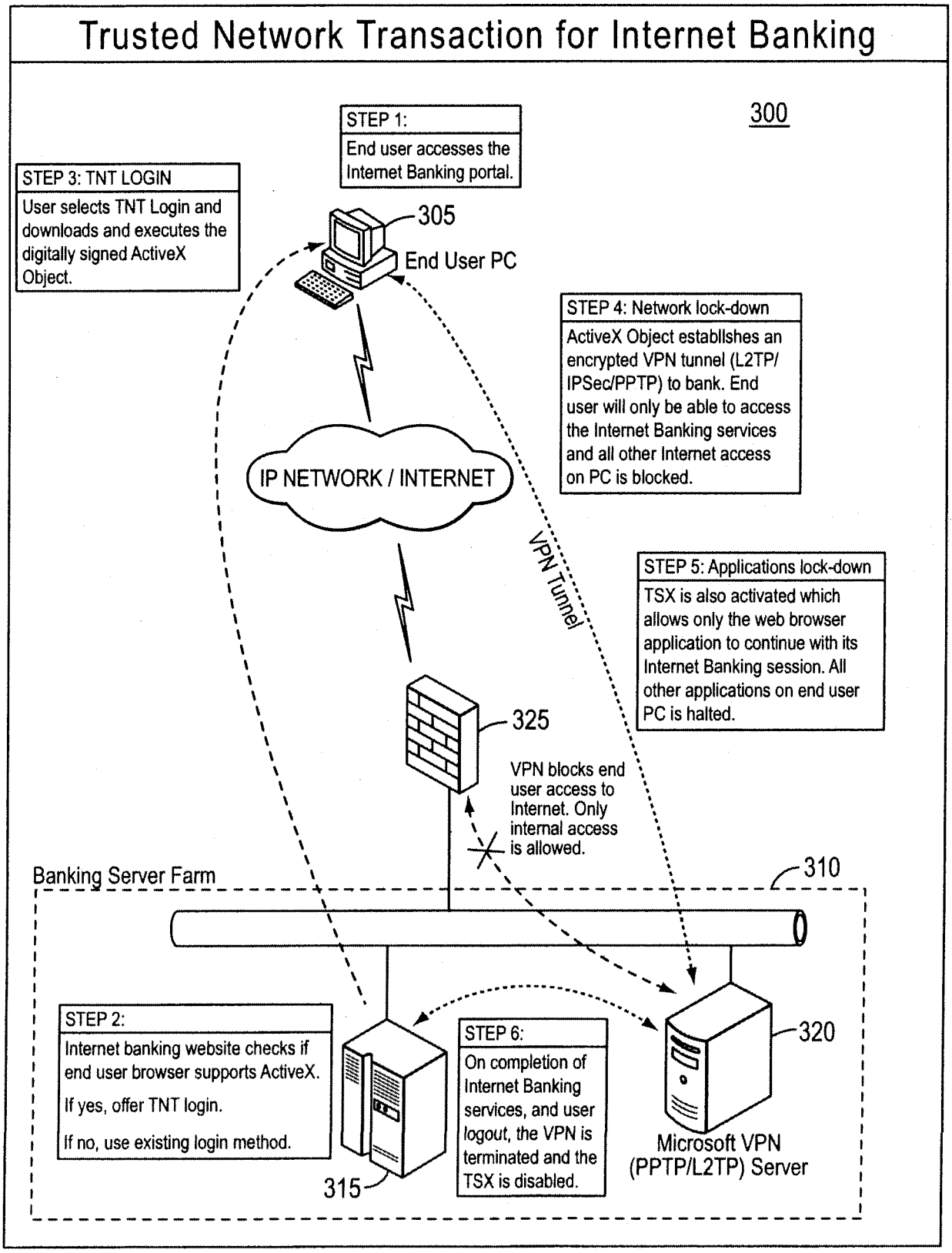

Trusted Network Transaction for Internet Banking
300
STEP 1:
End user accesses the Internet Banking portal.
STEP 3: TNT LOGIN
User selects TNT Login and downloads and executes the digitally signed ActiveX Object.
305
End User PC
STEP 4: Network lock-down
ActiveX Object establishes an encrypted VPN tunnel (L2TP/IPSec/PPTP) to bank. End user will only be able to access the Internet Banking services and all other Internet access on PC is blocked.
IP NETWORK / INTERNET
VPN Tunnel
STEP 5: Applications lock-down
TSX is also activated which allows only the web browser application to continue with its Internet Banking session. All other applications on end user PC is halted.
325
VPN blocks end user access to Internet. Only internal access is allowed.
Banking Server Farm
310
STEP 2:
Internet banking website checks if end user browser supports ActiveX.
If yes, offer TNT login.
If no, use existing login method.
315
STEP 6:
On completion of Internet Banking services, and user logout, the VPN is terminated and the TSX is disabled.
320
Microsoft VPN (PPTP/L2TP) Server

FIG. 3

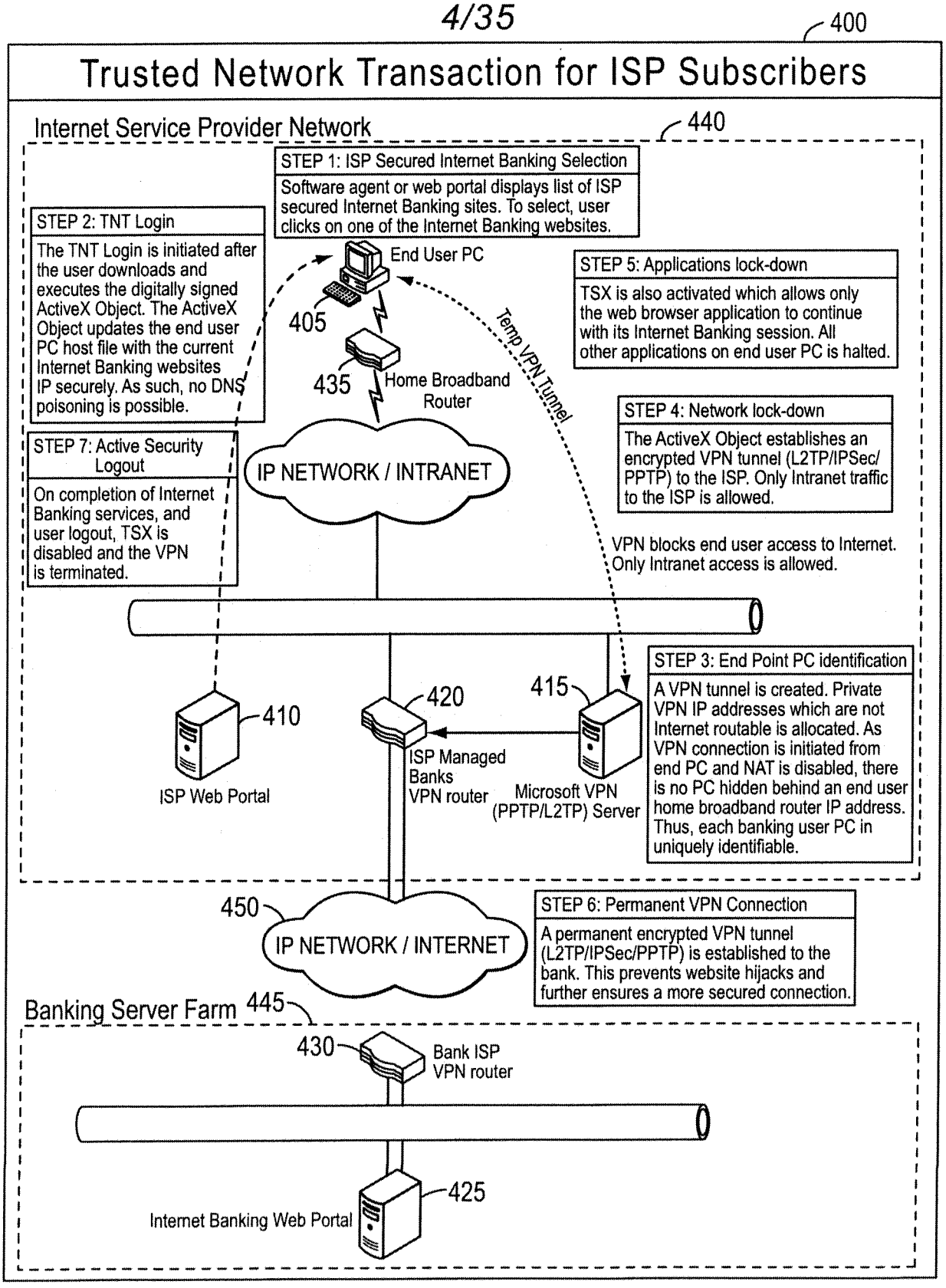

400
Trusted Network Transaction for ISP Subscribers
Internet Service Provider Network
440
STEP 1: ISP Secured Internet Banking Selection
Software agent or web portal displays list of ISP secured Internet Banking sites. To select, user clicks on one of the Internet Banking websites.
STEP 2: TNT Login
The TNT Login is initiated after the user downloads and executes the digitally signed ActiveX Object. The ActiveX Object updates the end user PC host file with the current Internet Banking websites IP securely. As such, no DNS poisoning is possible.
End User PC
405
435
Home Broadband Router
Temp VPN Tunnel
STEP 5: Applications lock-down
TSX is also activated which allows only the web browser application to continue with its Internet Banking session. All other applications on end user PC is halted.
STEP 4: Network lock-down
The ActiveX Object establishes an encrypted VPN tunnel (L2TP/IPSec/PPTP) to the ISP. Only Intranet traffic to the ISP is allowed.
IP NETWORK / INTRANET
STEP 7: Active Security Logout
On completion of Internet Banking services, and user logout, TSX is disabled and the VPN is terminated.
VPN blocks end user access to Internet. Only Intranet access is allowed.
410
ISP Web Portal
420
ISP Managed Banks VPN router
415
Microsoft VPN (PPTP/L2TP) Server
STEP 3: End Point PC identification
A VPN tunnel is created. Private VPN IP addresses which are not Internet routable is allocated. As VPN connection is initiated from end PC and NAT is disabled, there is no PC hidden behind an end user home broadband router IP address. Thus, each banking user PC in uniquely identifiable.
450
IP NETWORK / INTERNET
STEP 6: Permanent VPN Connection
A permanent encrypted VPN tunnel (L2TP/IPSec/PPTP) is established to the bank. This prevents website hijacks and further ensures a more secured connection.
Banking Server Farm
445
430
Bank ISP VPN router
425
Internet Banking Web Portal

FIG. 4

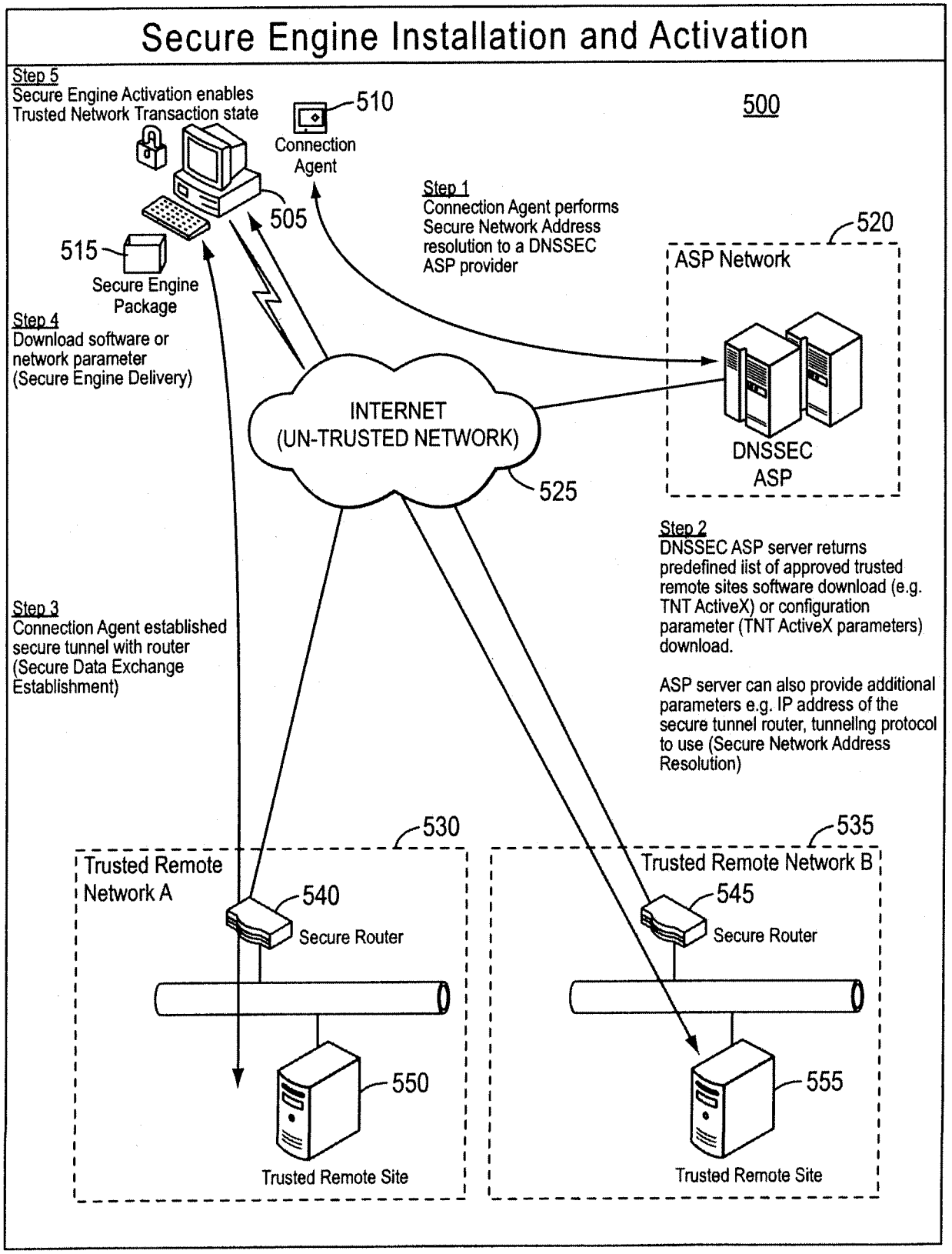
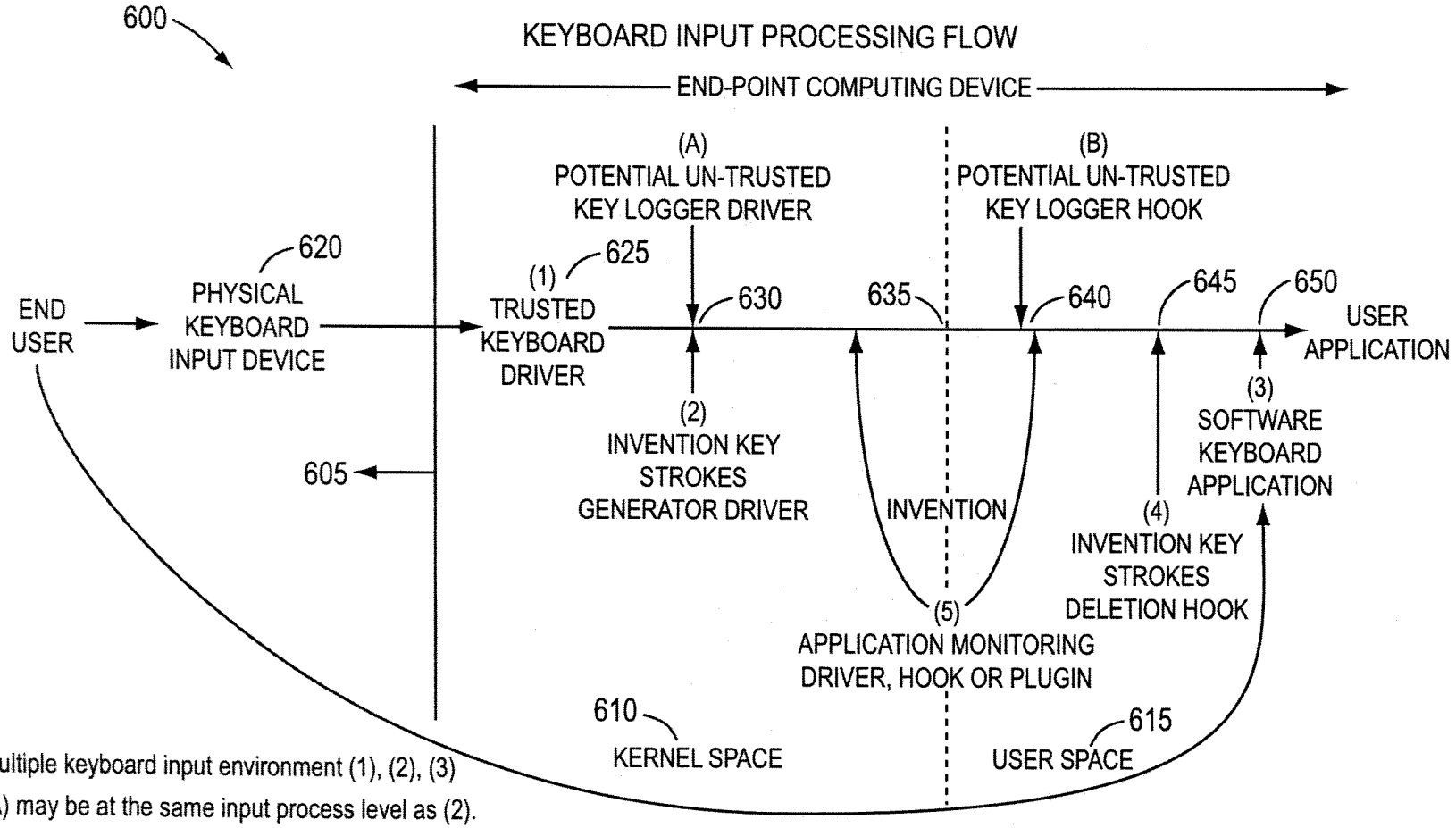

Secure Engine Installation and Activation
Step 5
Secure Engine Activation enables Trusted Network Transaction state
510
Connection Agent
500
505
515
Secure Engine Package
Step 1
Connection Agent performs Secure Network Address resolution to a DNSSEC ASP provider
520
ASP Network
Step 4
Download software or network parameter (Secure Engine Delivery)
INTERNET (UN-TRUSTED NETWORK)
525
DNSSEC ASP
Step 2
DNSSEC ASP server returns predefined list of approved trusted remote sites software download (e.g. TNT ActiveX) or configuration parameter (TNT ActiveX parameters) download.
ASP server can also provide additional parameters e.g. IP address of the secure tunnel router, tunnelling protocol to use (Secure Network Address Resolution)
Step 3
Connection Agent established secure tunnel with router (Secure Data Exchange Establishment)
530
Trusted Remote Network A
540
Secure Router
550
Trusted Remote Site
535
Trusted Remote Network B
545
Secure Router
555
Trusted Remote Site

FIG. 5



- Multiple keyboard input environment (1), (2), (3)
- (A) may be at the same input process level as (2). (A) cannot be at a lower input process level than (2)
- In the invention producer consumer model (4) must be after (B)
- In the invention standalone model (5) can be at any level (either kernel or user space) if the required application status information can be retrieved. (5) is independent of where (A) or (B) is installed.

FIG. 6

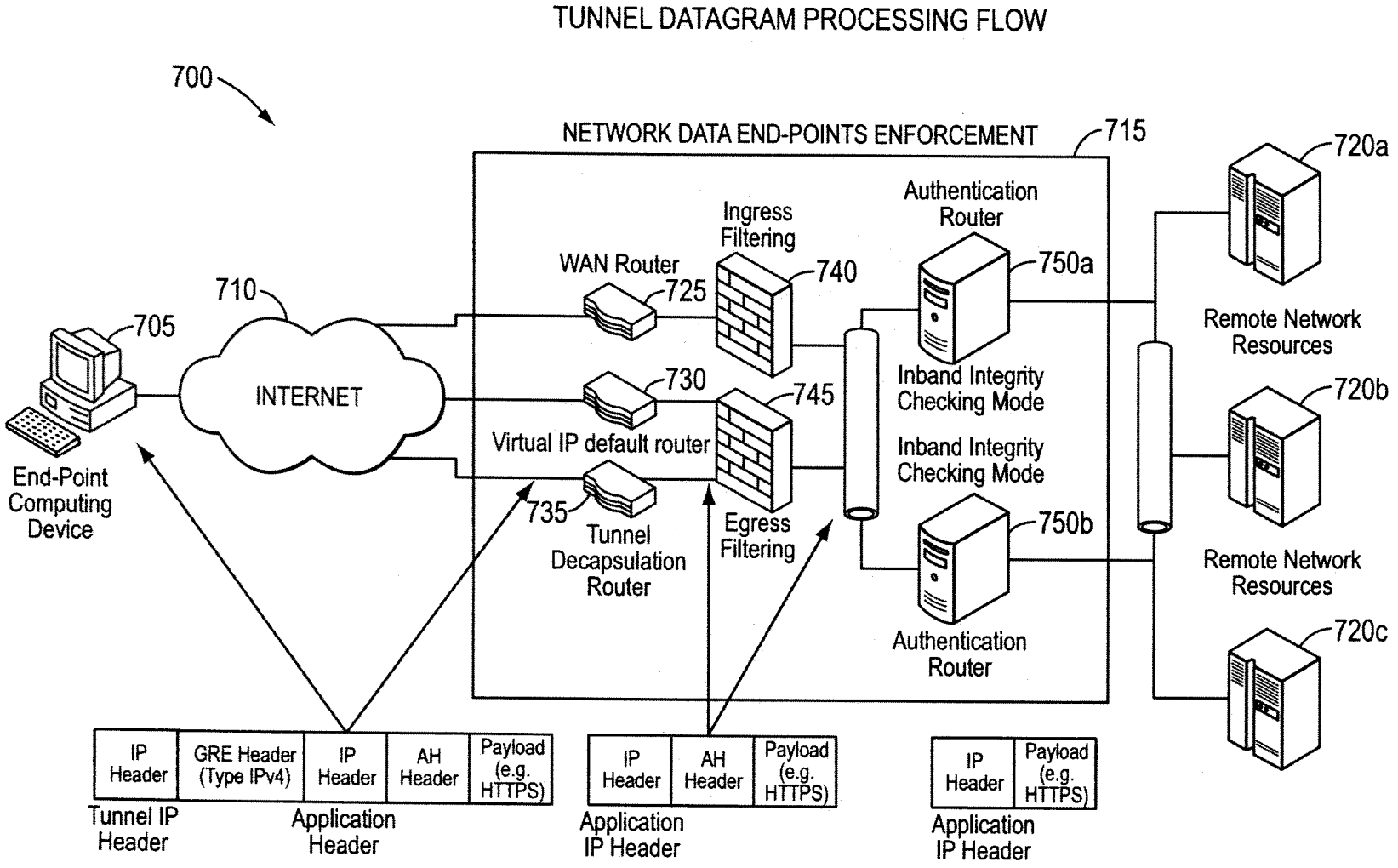

TUNNEL DATAGRAM PROCESSING FLOW
700
NETWORK DATA END-POINTS ENFORCEMENT
715
720a
Authentication Router
Ingress Filtering
WAN Router
725
740
750a
710
705
INTERNET
730
745
Virtual IP default router
Inband Integrity Checking Mode
Remote Network Resources
720b
Inband Integrity Checking Mode
End-Point Computing Device
735
Tunnel Decapsulation Router
Egress Filtering
750b
Remote Network Resources
Authentication Router
720c
IP Header
GRE Header (Type IPv4)
IP Header
AH Header
Payload (e.g. HTTPS)
Tunnel IP Header
Application Header
IP Header
AH Header
Payload (e.g. HTTPS)
Application IP Header
IP Header
Payload (e.g. HTTPS)
Application IP Header

FIG. 7

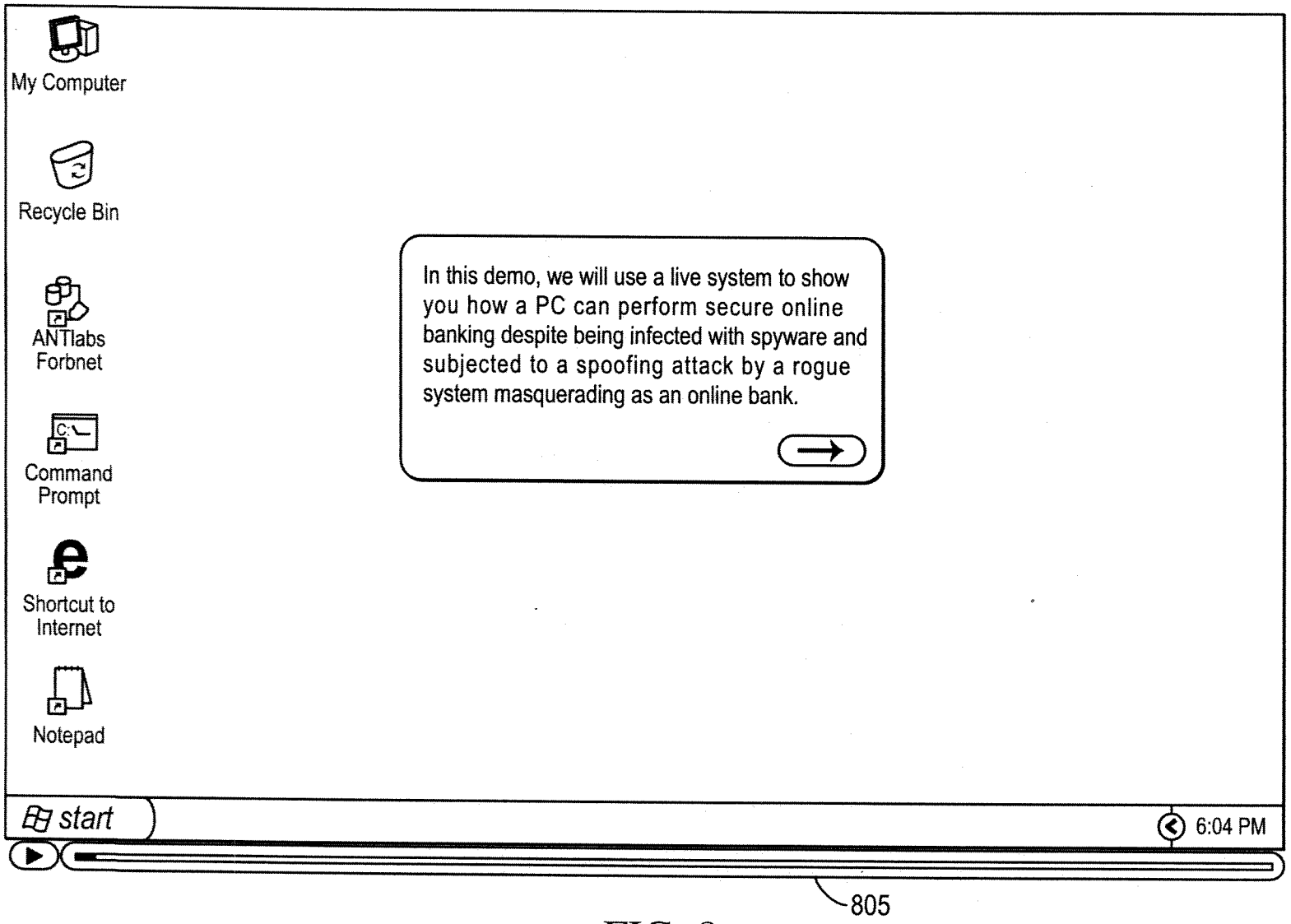

My Computer
Recycle Bin
ANTIabs Forbnet
Command Prompt
Shortcut to Internet
Notepad
In this demo, we will use a live system to show you how a PC can perform secure online banking despite being infected with spyware and subjected to a spoofing attack by a rogue system masquerading as an online bank.
start
6:04 PM
805

FIG. 8

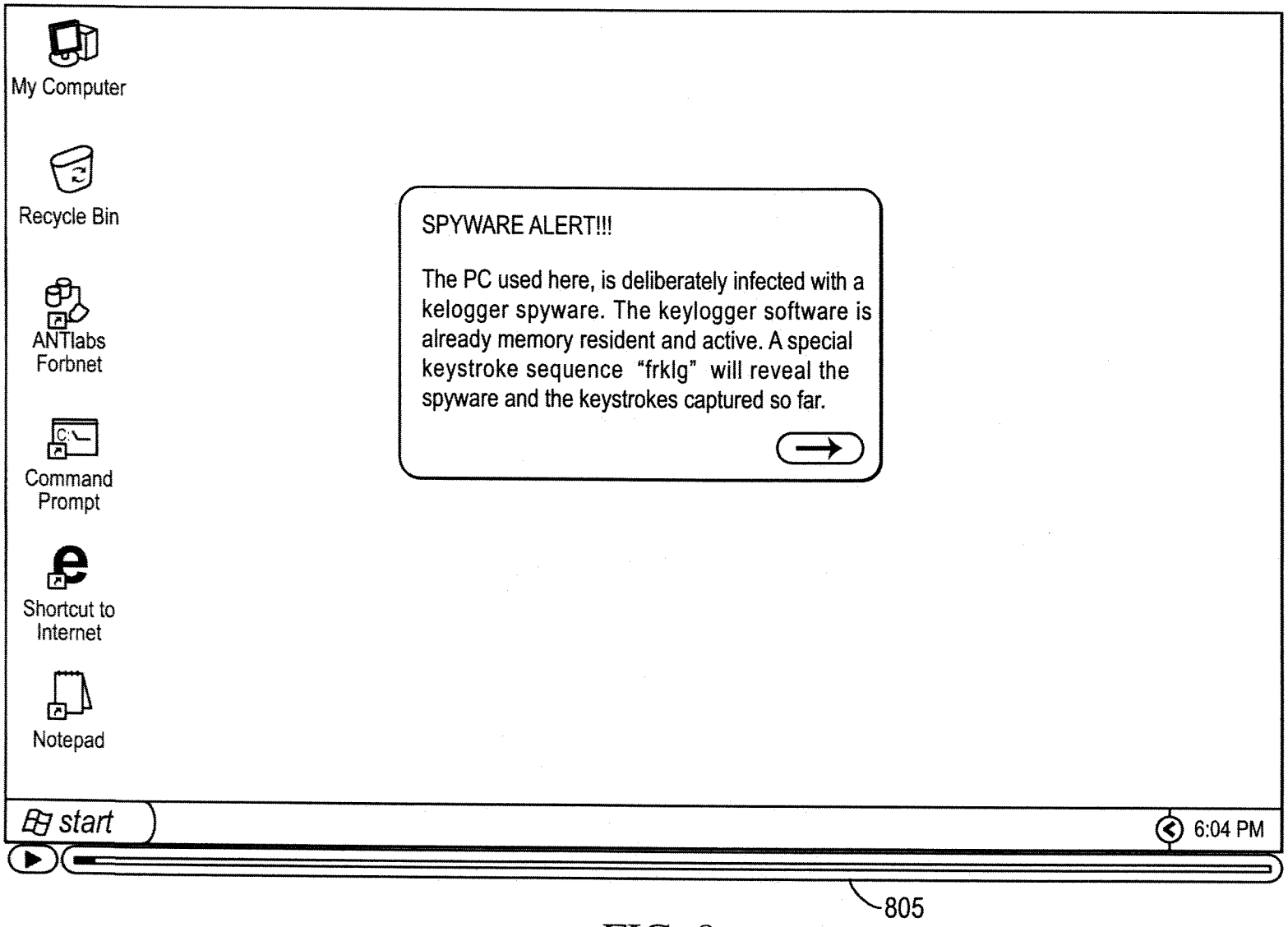

My Computer
Recycle Bin
ANTIabs Forbnet
Command Prompt
Shortcut to Internet
Notepad
SPYWARE ALERT!!!
The PC used here, is deliberately infected with a kelogger spyware. The keylogger software is already memory resident and active. A special keystroke sequence "frklg" will reveal the spyware and the keystrokes captured so far.
start
6:04 PM
805

FIG. 9

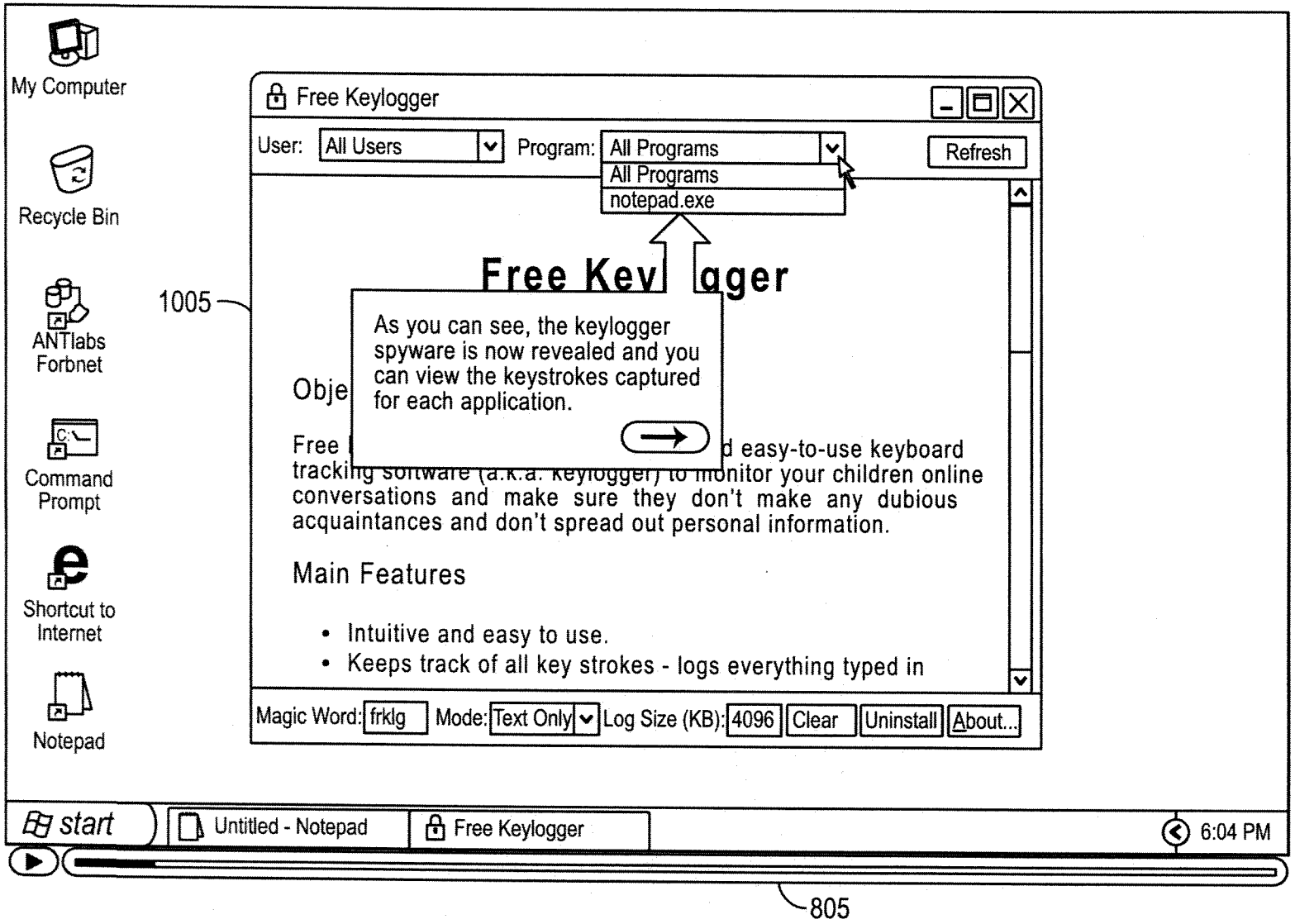

My Computer
Recycle Bin
ANTIabs Forbnet
Command Prompt
Shortcut to Internet
Notepad
1005
Free Keylogger
User: All Users
Program: All Programs
All Programs
notepad.exe
Refresh
Free Key gger
As you can see, the keylogger spyware is now revealed and you can view the keystrokes captured for each application.
Obje
Free d easy-to-use keyboard tracking software (a.k.a. keylogger) to monitor your children online conversations and make sure they don't make any dubious acquaintances and don't spread out personal information.
Main Features
• Intuitive and easy to use.
• Keeps track of all key strokes - logs everything typed in
Magic Word: frklg
Mode: Text Only
Log Size (KB): 4096
Clear
Uninstall
About...
start
Untitled - Notepad
Free Keylogger
6:04 PM
805

FIG. 10

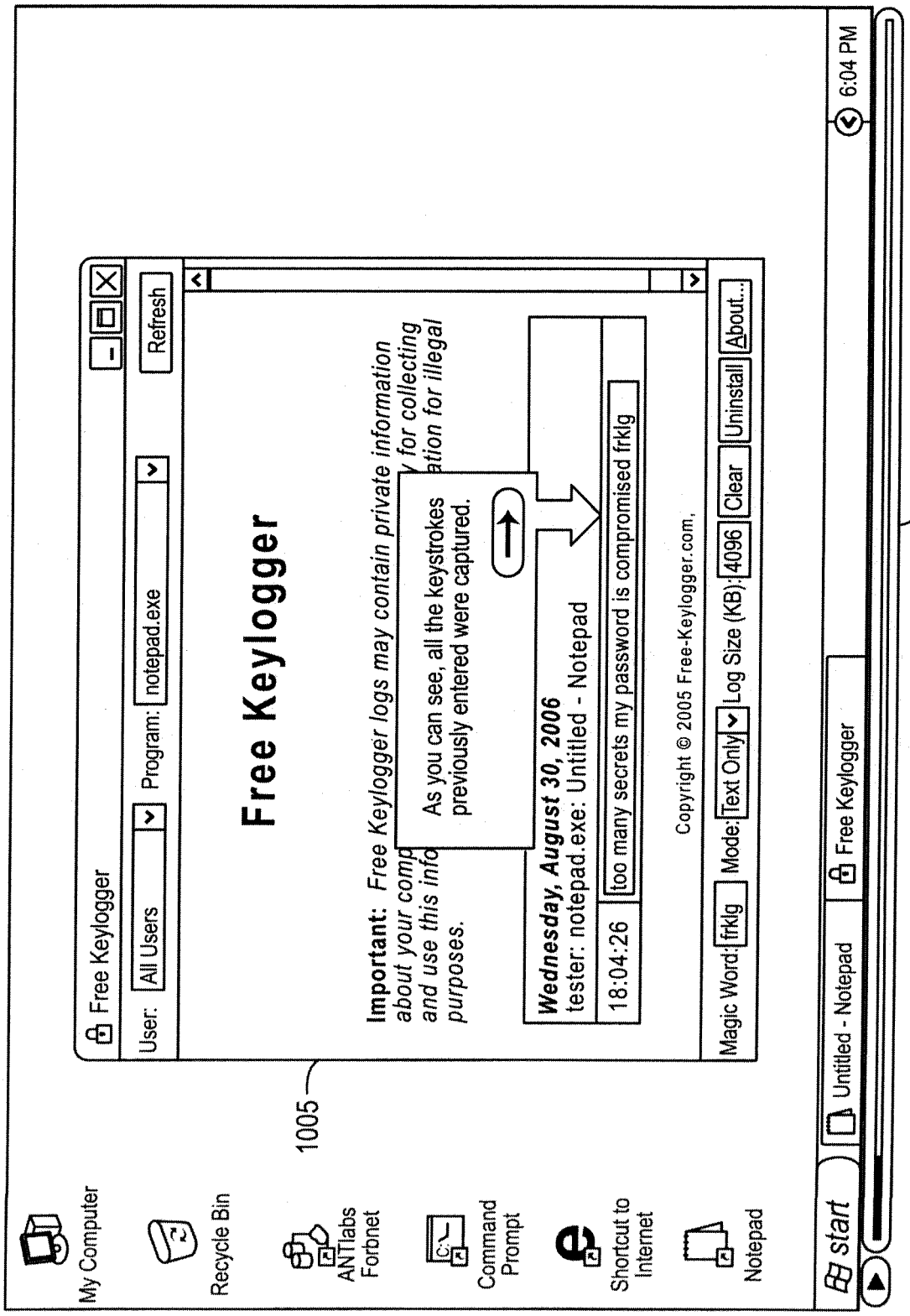

My Computer
Recycle Bin
ANTlabs Forbnet
Command Prompt
Shortcut to Internet
Notepad
Free Keylogger
User: All Users
Program: notepad.exe
Refresh
Free Keylogger
Important: Free Keylogger logs may contain private information about your comp
y for collecting
and use this info
ation for illegal
purposes.
As you can see, all the keystrokes previously entered were captured.
Wednesday, August 30, 2006
tester: notepad.exe: Untitled - Notepad
18:04:26
too many secrets my password is compromised frklg
Copyright © 2005 Free-Keylogger.com,
Magic Word: frklg
Mode: Text Only
Log Size (KB): 4096
Clear
Uninstall
About...
1005
805
start
Untitled - Notepad
Free Keylogger
6:04 PM

FIG. 11

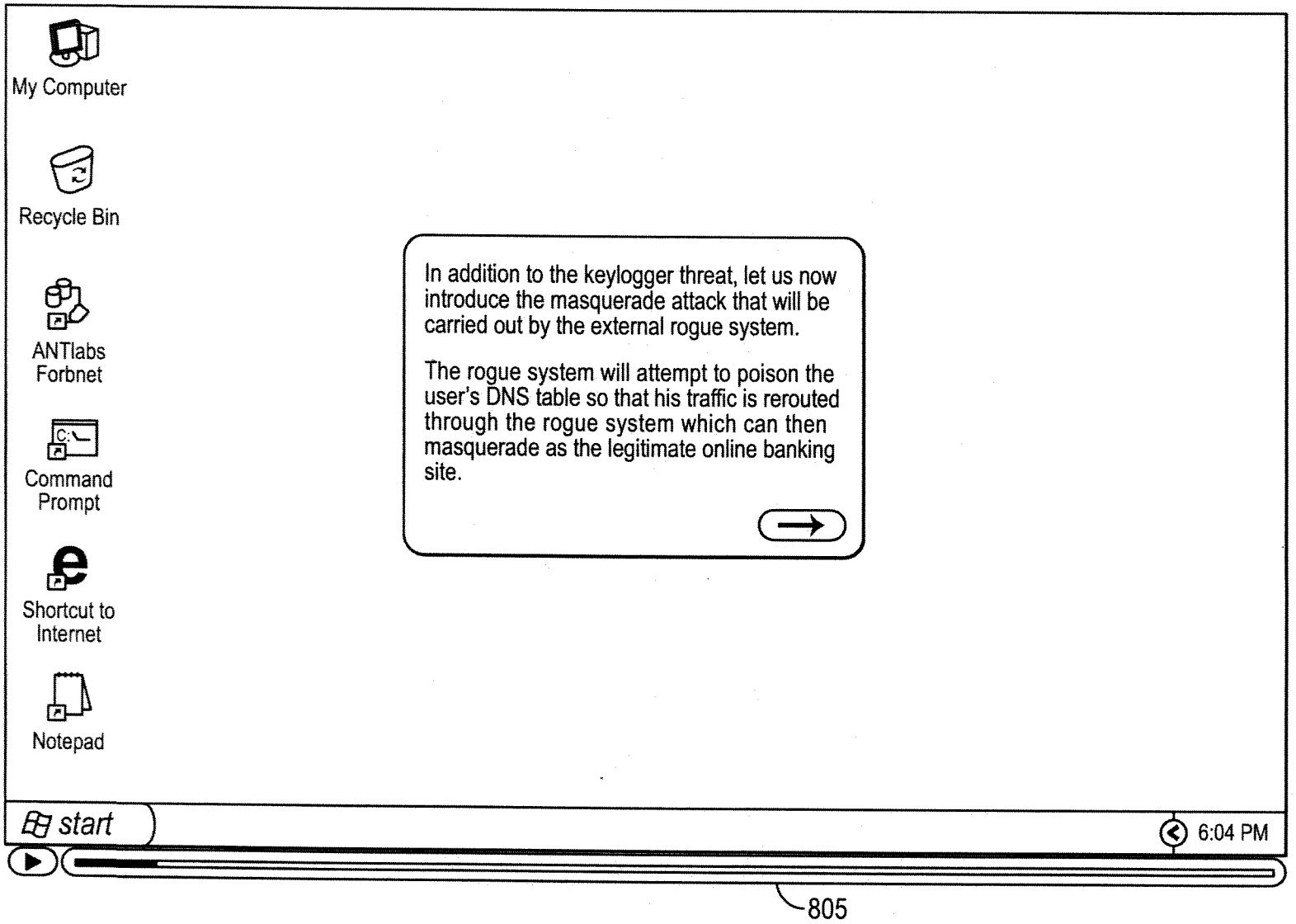

My Computer
Recycle Bin
ANTlabs Forbnet
Command Prompt
Shortcut to Internet
Notepad
In addition to the keylogger threat, let us now introduce the masquerade attack that will be carried out by the external rogue system.
The rogue system will attempt to poison the user's DNS table so that his traffic is rerouted through the rogue system which can then masquerade as the legitimate online banking site.
start
6:04 PM
805

FIG. 12

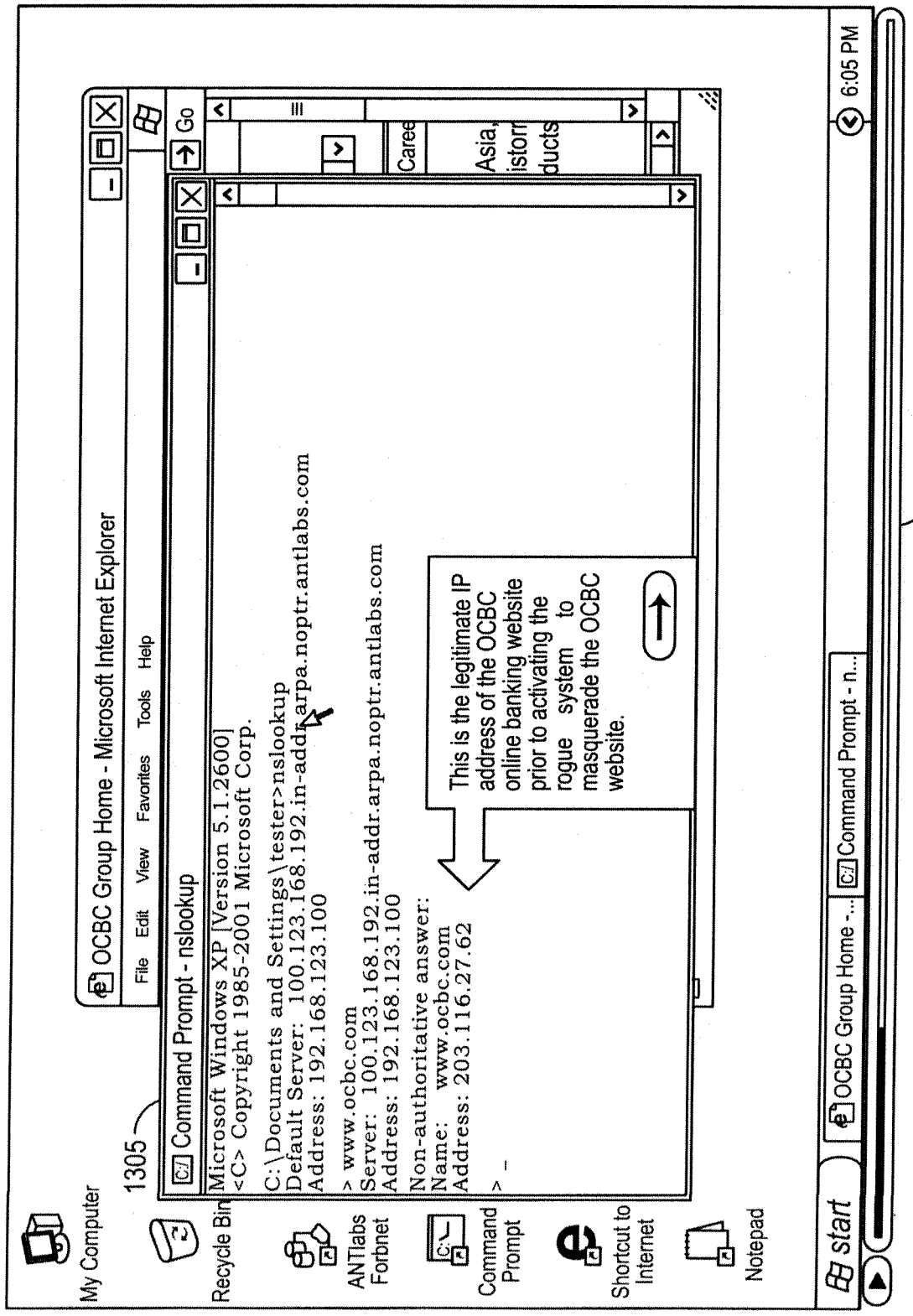

My Computer
Recycle Bin
ANTlabs Forbnet
Command Prompt
Shortcut to Internet
Notepad
OCBC Group Home - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Go
Command Prompt - nslookup
Microsoft Windows XP [Version 5.1.2600]
<C> Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\tester>nslookup
Default Server: 100.123.168.192.in-addr.arpa.noptr.antlabs.com
Address: 192.168.123.100
> www.ocbc.com
Server: 100.123.168.192.in-addr.arpa.noptr.antlabs.com
Address: 192.168.123.100
Non-authoritative answer:
Name: www.ocbc.com
Address: 203.116.27.62
> _
This is the legitimate IP address of the OCBC online banking website prior to activating the rogue system to masquerade the OCBC website.
1305
805
start
OCBC Group Home -...
Command Prompt - n...
6:05 PM

FIG. 13

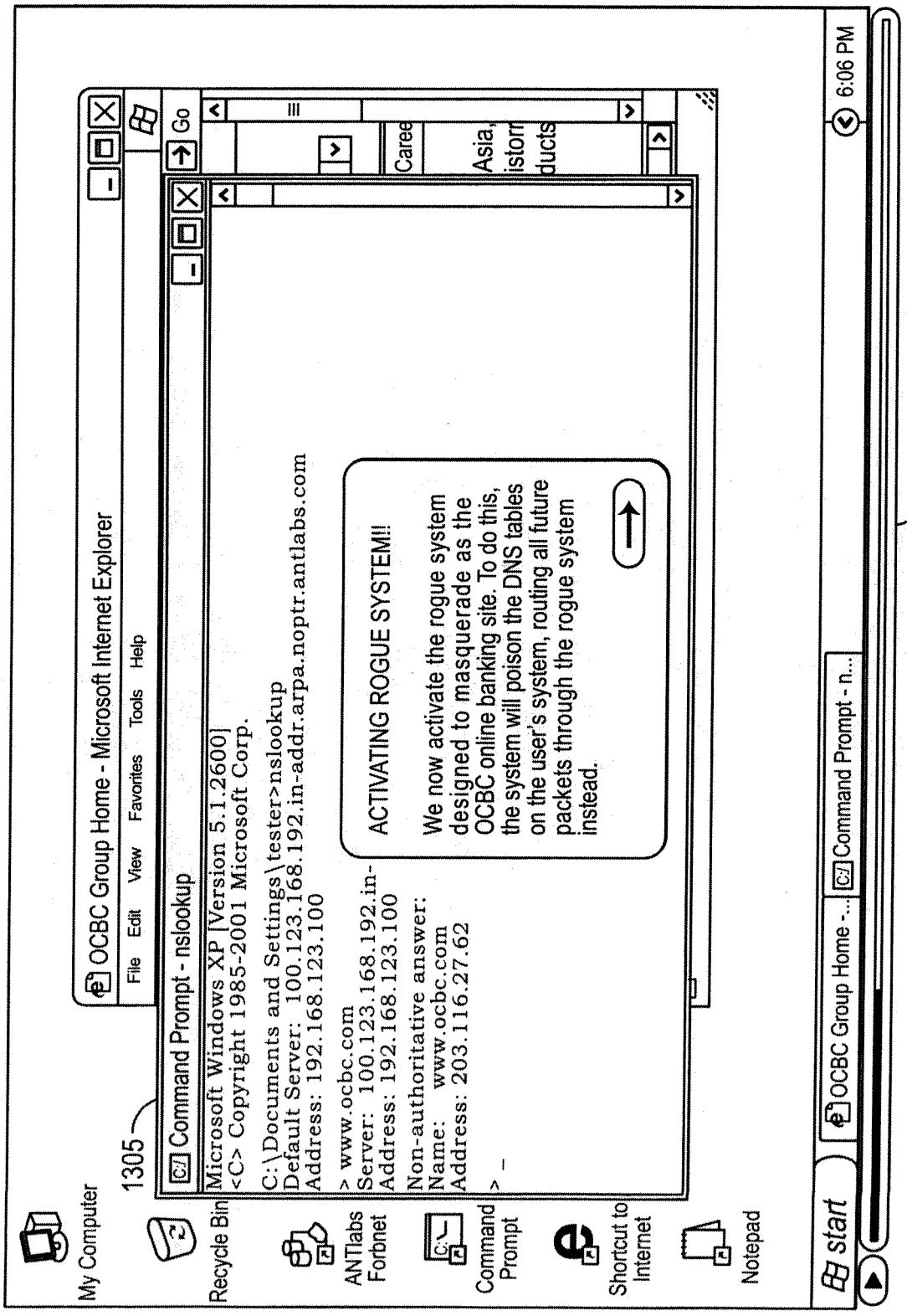

My Computer
Recycle Bin
ANTlabs Forbnet
Command Prompt
Shortcut to Internet
Notepad
1305
OCBC Group Home - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Go
Command Prompt - nslookup
Microsoft Windows XP [Version 5.1.2600]
<C> Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\tester>nslookup
Default Server: 100.123.168.192.in-addr.arpa.noptr.antlabs.com
Address: 192.168.123.100
> www.ocbc.com
Server: 100.123.168.192.in-
Address: 192.168.123.100
Non-authoritative answer:
Name: www.ocbc.com
Address: 203.116.27.62
> _
ACTIVATING ROGUE SYSTEM!!
We now activate the rogue system designed to masquerade as the OCBC online banking site. To do this, the system will poison the DNS tables on the user's system, routing all future packets through the rogue system instead.
Caree
Asia,
istorr
ducts
start
OCBC Group Home -...
Command Prompt - n...
6:06 PM
805

FIG. 14

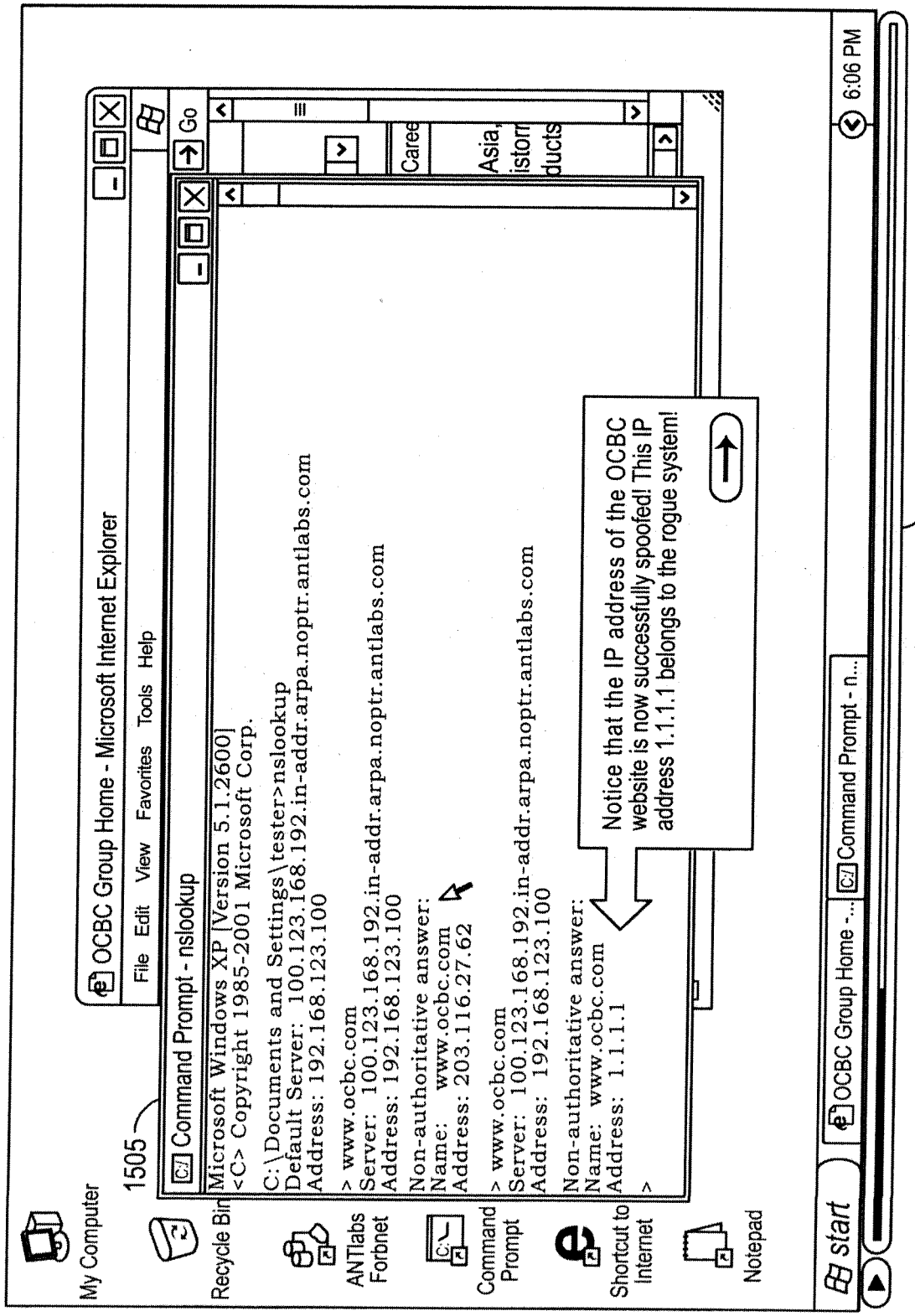

My Computer
Recycle Bin
ANTlabs Forbnet
Command Prompt
Shortcut to Internet
Notepad
1505
OCBC Group Home - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Go
Command Prompt - nslookup
Microsoft Windows XP [Version 5.1.2600]
<C> Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\tester>nslookup
Default Server: 100.123.168.192.in-addr.arpa.noptr.antlabs.com
Address: 192.168.123.100
> www.ocbc.com
Server: 100.123.168.192.in-addr.arpa.noptr.antlabs.com
Address: 192.168.123.100
Non-authoritative answer:
Name: www.ocbc.com
Address: 203.116.27.62
> www.ocbc.com
Server: 100.123.168.192.in-addr.arpa.noptr.antlabs.com
Address: 192.168.123.100
Non-authoritative answer:
Name: www.ocbc.com
Address: 1.1.1.1
>
Notice that the IP address of the OCBC website is now successfully spoofed! This IP address 1.1.1.1 belongs to the rogue system!
start
OCBC Group Home -...
Command Prompt - n...
6:06 PM
805

FIG. 15

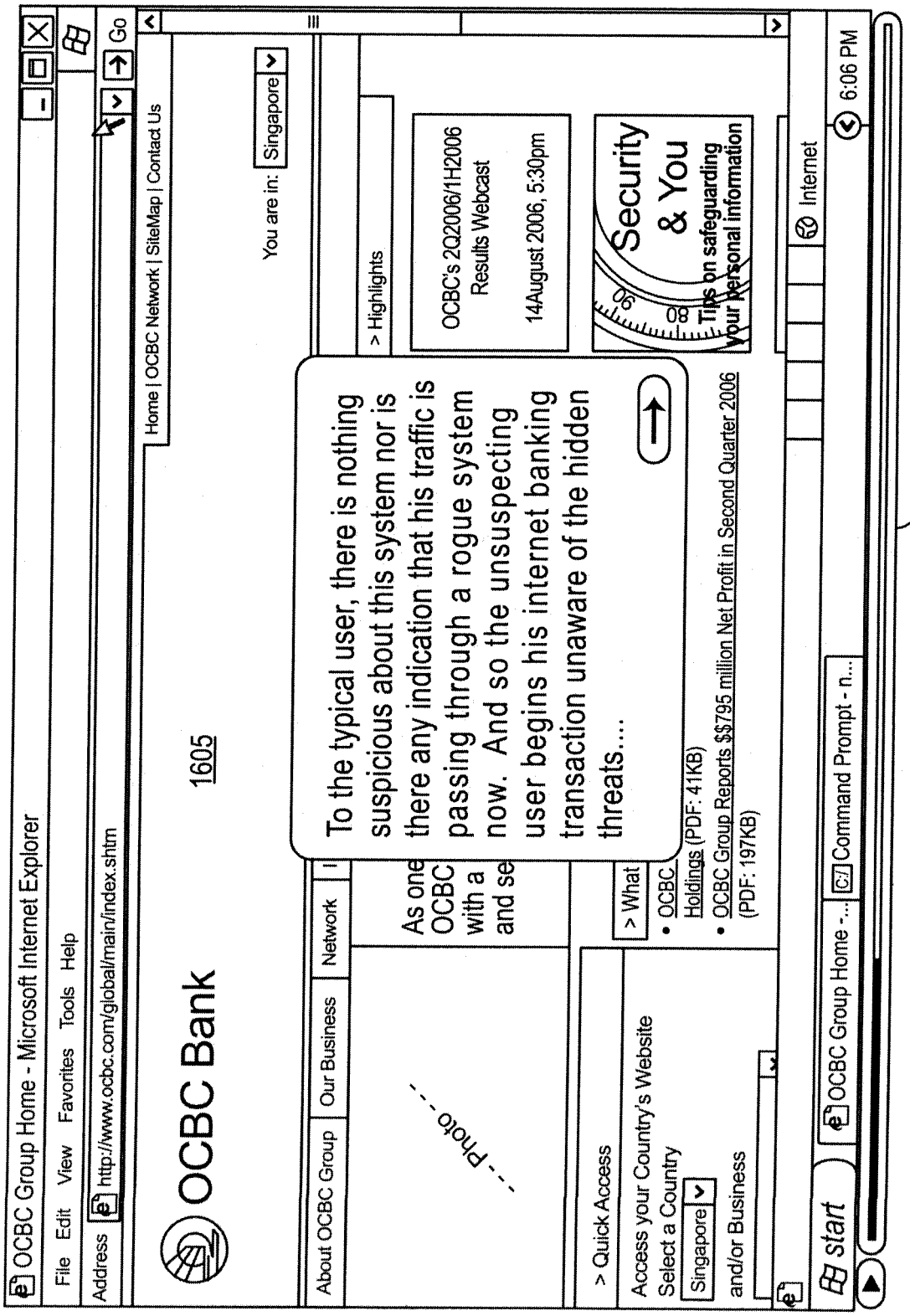

OCBC Group Home - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://www.ocbc.com/global/main/index.shtm
Go
OCBC Bank
1605
Home | OCBC Network | SiteMap | Contact Us
You are in: Singapore
About OCBC Group
Our Business
Network
Photo
As one OCBC with a and se
To the typical user, there is nothing suspicious about this system nor is there any indication that his traffic is passing through a rogue system now. And so the unsuspecting user begins his internet banking transaction unaware of the hidden threats....
> Highlights
OCBC's 2Q2006/1H2006 Results Webcast
14August 2006, 5:30pm
Security & You
Tips on safeguarding your personal information
> Quick Access
Access your Country's Website
Select a Country
Singapore
and/or Business
> What
OCBC Holdings (PDF: 41KB)
OCBC Group Reports $795 million Net Profit in Second Quarter 2006 (PDF: 197KB)
start
OCBC Group Home -...
Command Prompt - n...
Internet
6:06 PM
805

FIG. 16

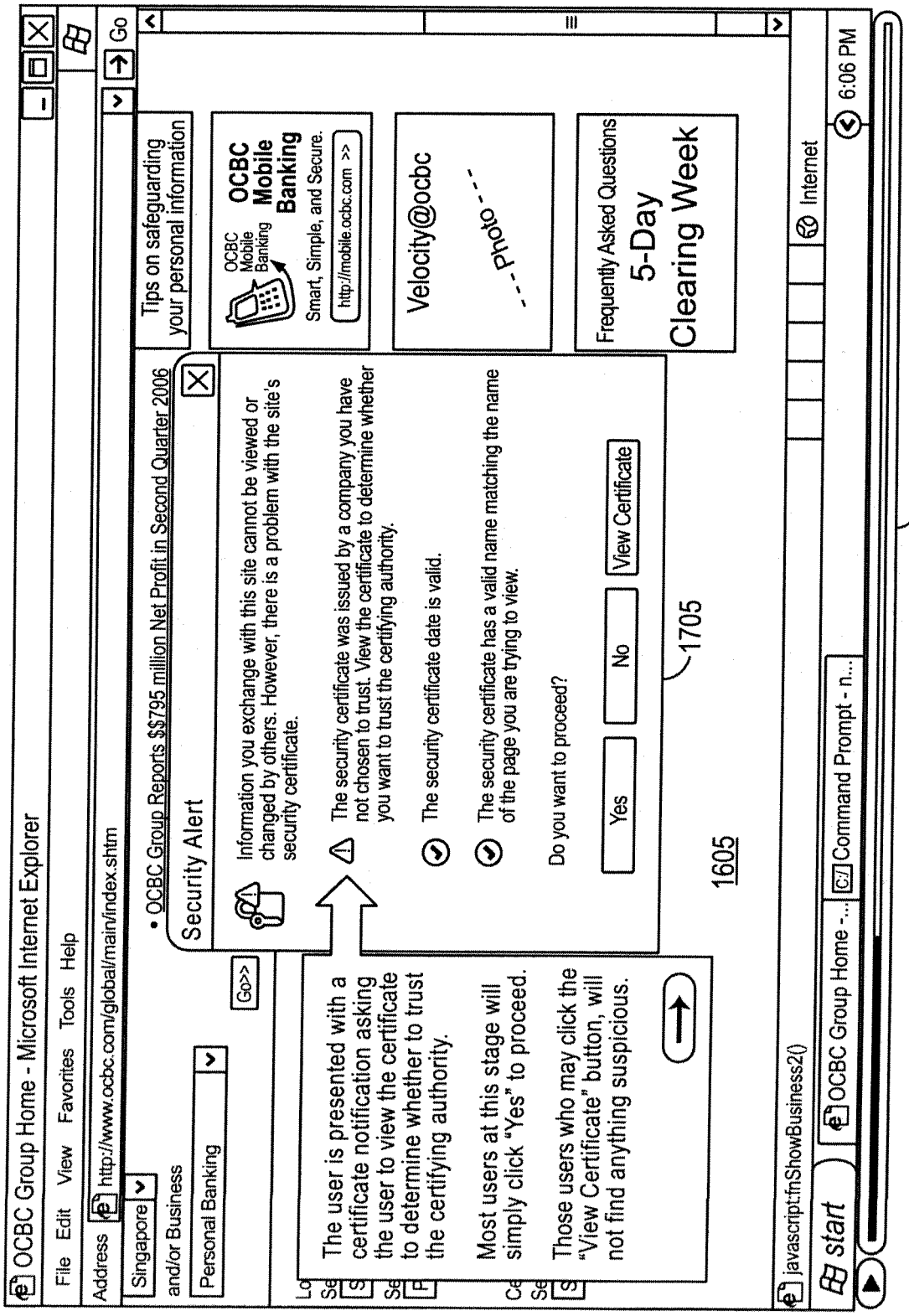

OCBC Group Home - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://www.ocbc.com/global/main/index.shtm
Go
Singapore
and/or Business
Personal Banking
Go>>
• OCBC Group Reports $$795 million Net Profit in Second Quarter 2006
Tips on safeguarding your personal information
OCBC Mobile Banking
Smart, Simple, and Secure.
http://mobile.ocbc.com >>
Velocity@ocbc
---Photo---
Frequently Asked Questions
5-Day Clearing Week
Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The security certificate has a valid name matching the name of the page you are trying to view.
Do you want to proceed?
Yes
No
View Certificate
1705
1605
The user is presented with a certificate notification asking the user to view the certificate to determine whether to trust the certifying authority.
Most users at this stage will simply click "Yes" to proceed.
Those users who may click the "View Certificate" button, will not find anything suspicious.
javascript:fnShowBusiness2()
start
OCBC Group Home -...
Command Prompt - n...
Internet
6:06 PM
805

FIG. 17

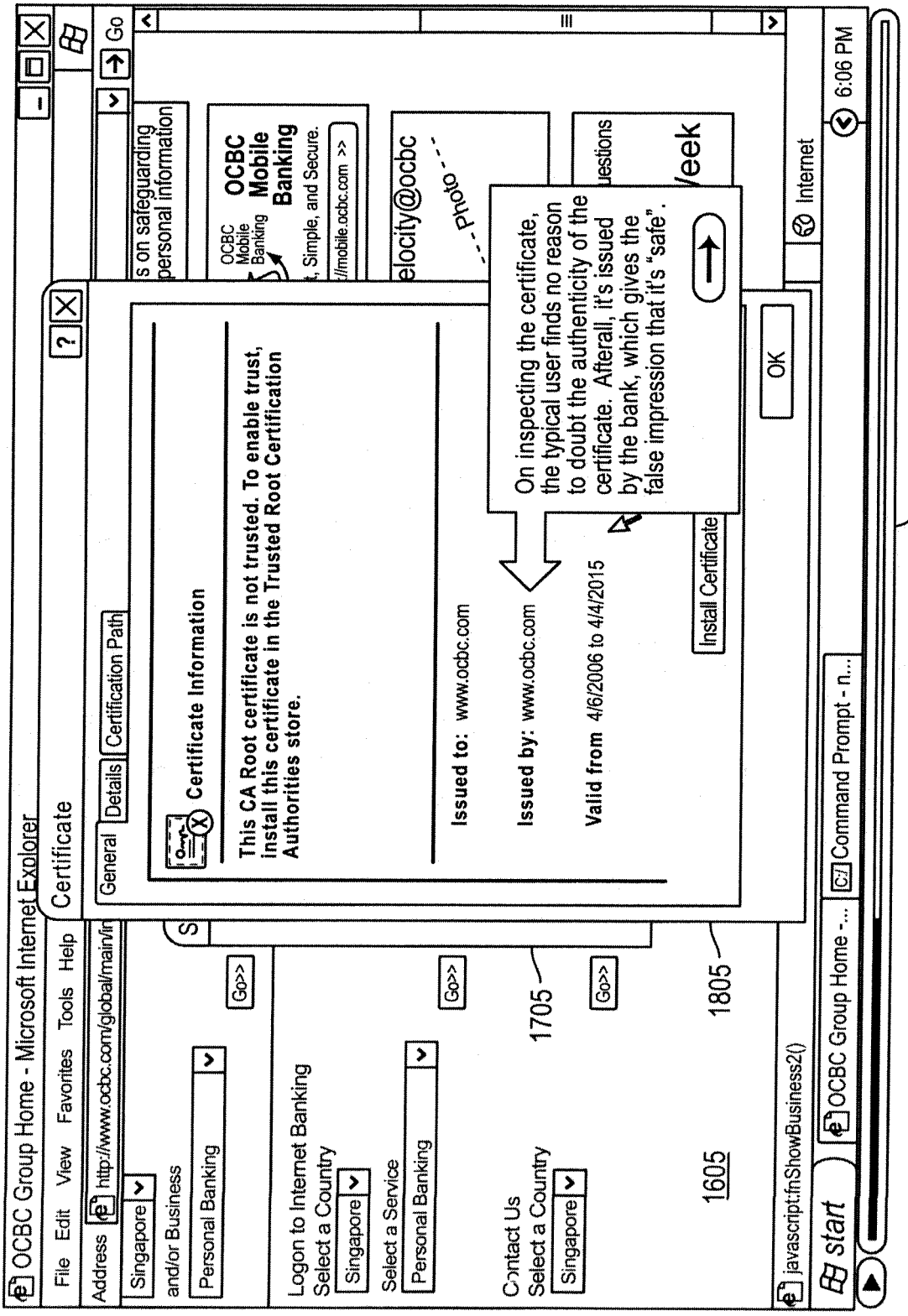

OCBC Group Home - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://www.ocbc.com/global/main/in
Singapore
and/or Business
Personal Banking
Go>>
Logon to Internet Banking
Select a Country
Singapore
Select a Service
Personal Banking
Go>>
Contact Us
Select a Country
Singapore
Go>>
1705
1605
1805
javascript:fnShowBusiness2()
start
OCBC Group Home -...
Command Prompt - n...
6:06 PM
Certificate
General
Details
Certification Path
Certificate Information
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.
Issued to: www.ocbc.com
Issued by: www.ocbc.com
Valid from 4/6/2006 to 4/4/2015
Install Certificate
OK
On inspecting the certificate, the typical user finds no reason to doubt the authenticity of the certificate. Afterall, it's issued by the bank, which gives the false impression that it's "safe".
OCBC Mobile Banking
Simple, and Secure.
Internet
805

FIG. 18

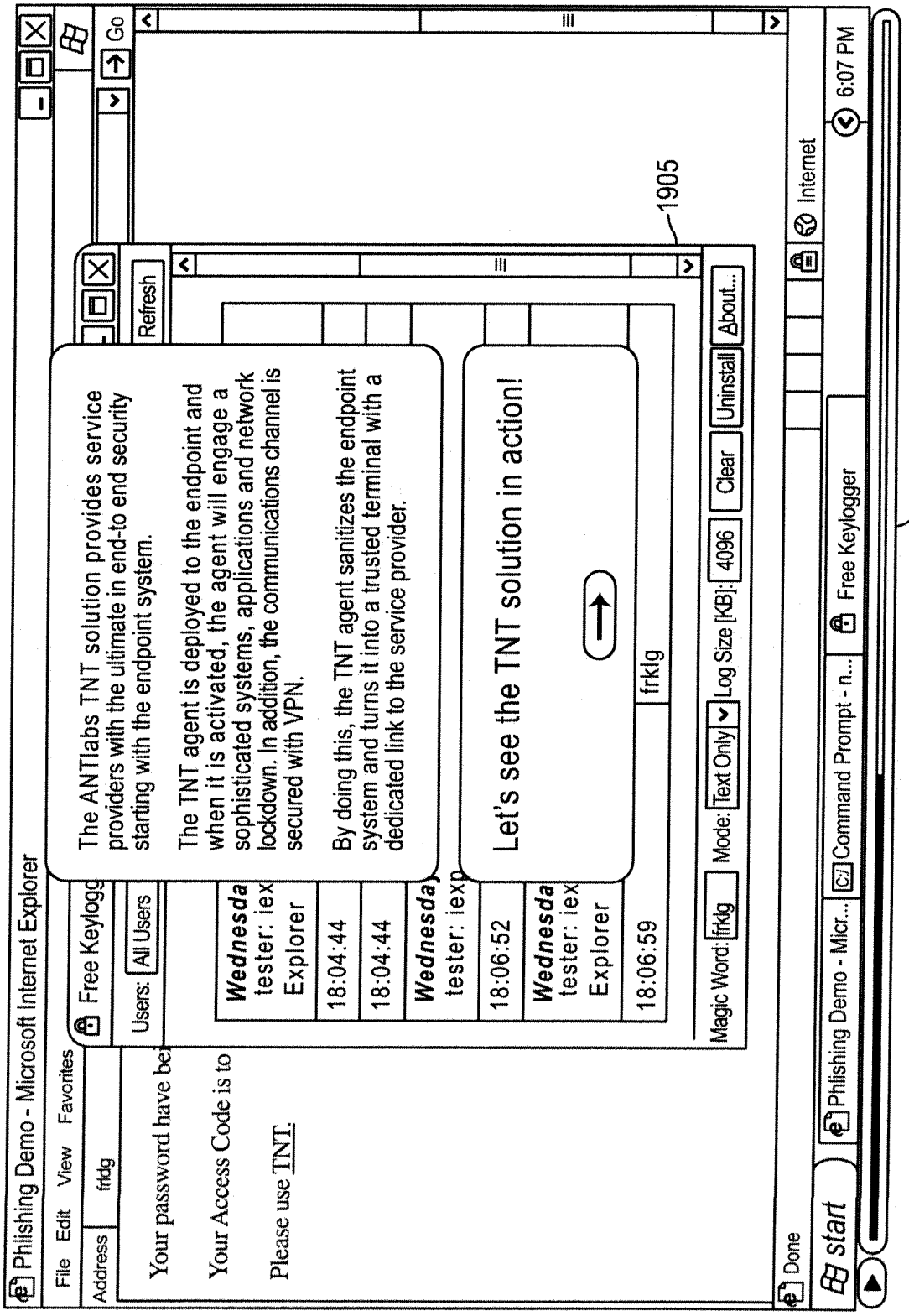

Phlishing Demo - Microsoft Internet Explorer
File Edit View Favorites
Address frkdg
Free Keylogg
Users: All Users
Your password have be
Your Access Code is to
Please use TNT.
Wednesda
tester: iex
Explorer
18:04:44
18:04:44
Wednesda
tester: iexp
18:06:52
Wednesda
tester: iex
Explorer
18:06:59
frklg
The ANTIabs TNT solution provides service providers with the ultimate in end-to end security starting with the endpoint system.
The TNT agent is deployed to the endpoint and when it is activated, the agent will engage a sophisticated systems, applications and network lockdown. In addition, the communications channel is secured with VPN.
By doing this, the TNT agent sanitizes the endpoint system and turns it into a trusted terminal with a dedicated link to the service provider.
Let's see the TNT solution in action!
Refresh
Magic Word: frkdg
Mode: Text Only
Log Size [KB]: 4096
Clear
Uninstall
About...
1905
Done
Internet
start
Phlishing Demo - Micr...
Command Prompt - n...
Free Keylogger
6:07 PM
805

FIG. 19

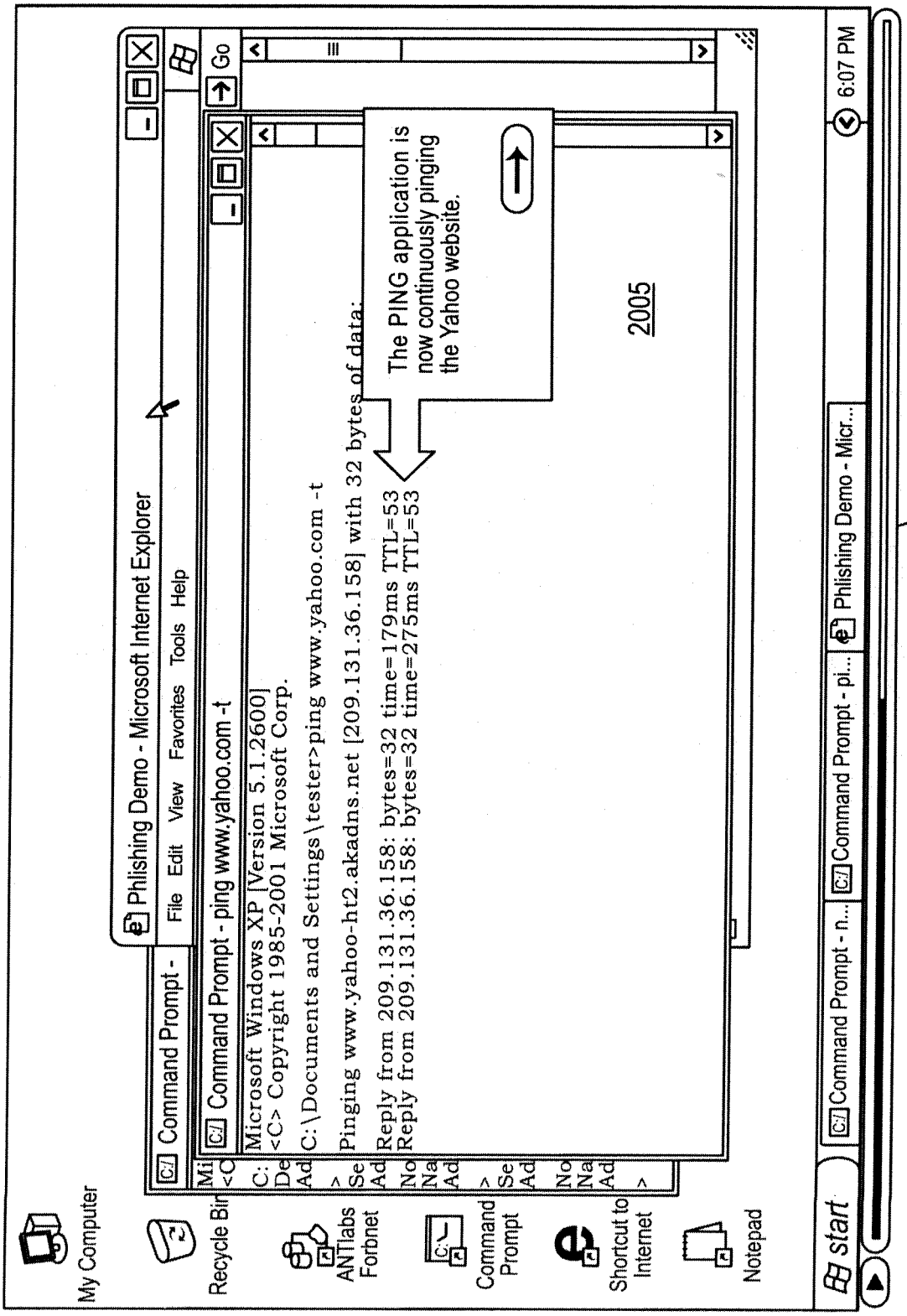

Phishing Demo - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Command Prompt - ping www.yahoo.com -t
Microsoft Windows XP [Version 5.1.2600]
<C> Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\tester>ping www.yahoo.com -t
Pinging www.yahoo-ht2.akadns.net [209.131.36.158] with 32 bytes of data:
Reply from 209.131.36.158: bytes=32 time=179ms TTL=53
Reply from 209.131.36.158: bytes=32 time=275ms TTL=53
The PING application is now continuously pinging the Yahoo website.
2005
My Computer
Recycle Bin
ANTlabs Forbnet
Command Prompt
Shortcut to Internet
Notepad
start
Command Prompt - n...
Command Prompt - pi...
Phishing Demo - Micr...
6:07 PM
805

FIG. 20

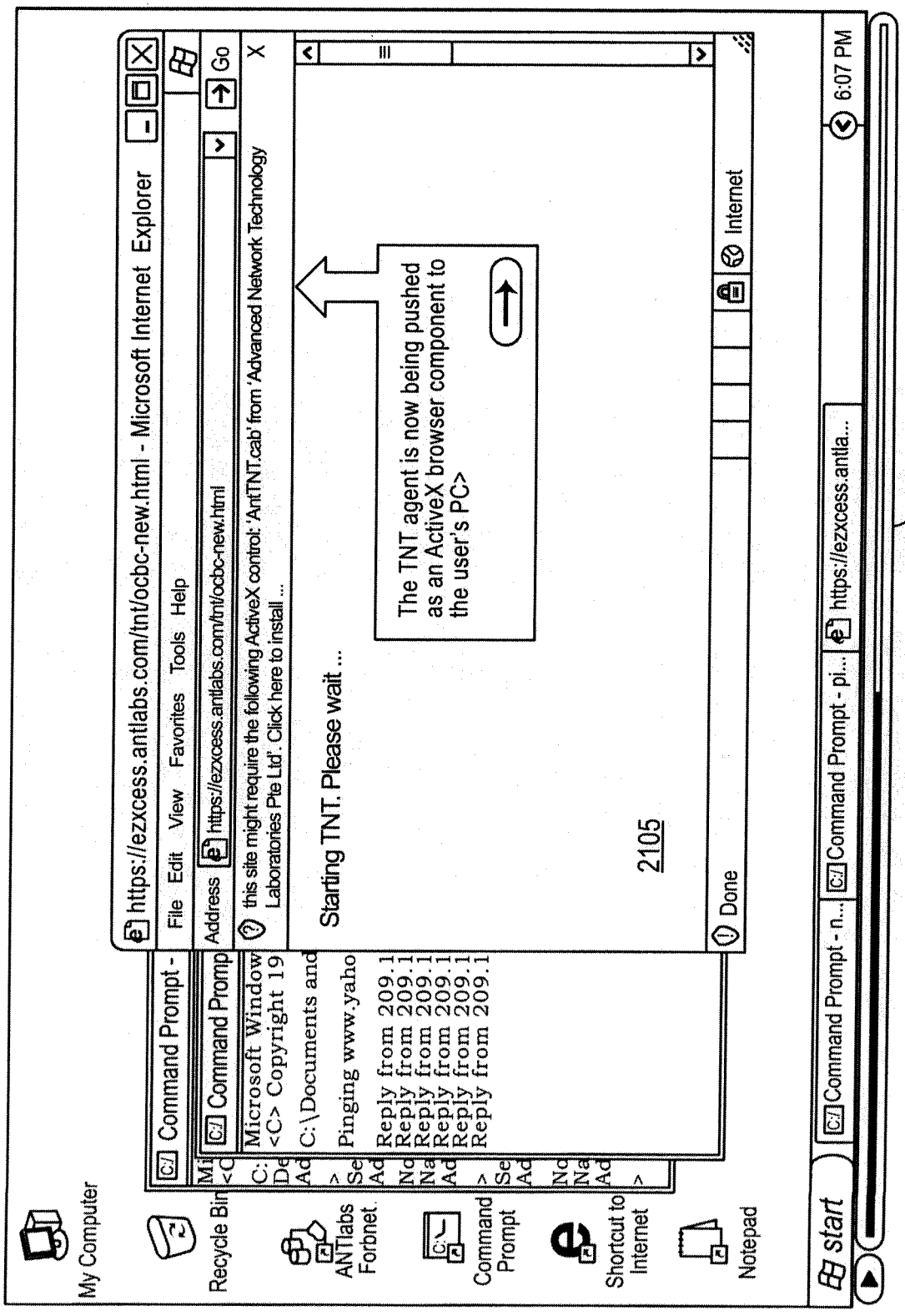

My Computer
Recycle Bin
ANTlabs Forbnet
Command Prompt
Shortcut to Internet
Notepad
https://ezxcess.antlabs.com/tnt/ocbc-new.html - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://ezxcess.antlabs.com/tnt/ocbc-new.html
Go
this site might require the following ActiveX control: 'AntTNT.cab' from 'Advanced Network Technology Laboratories Pte Ltd'. Click here to install ...
Starting TNT. Please wait ...
The TNT agent is now being pushed as an ActiveX browser component to the user's PC>
2105
Done
Internet
start
Command Prompt - n...
Command Prompt - pi...
https://ezxcess.antla...
6:07 PM
805

FIG. 21

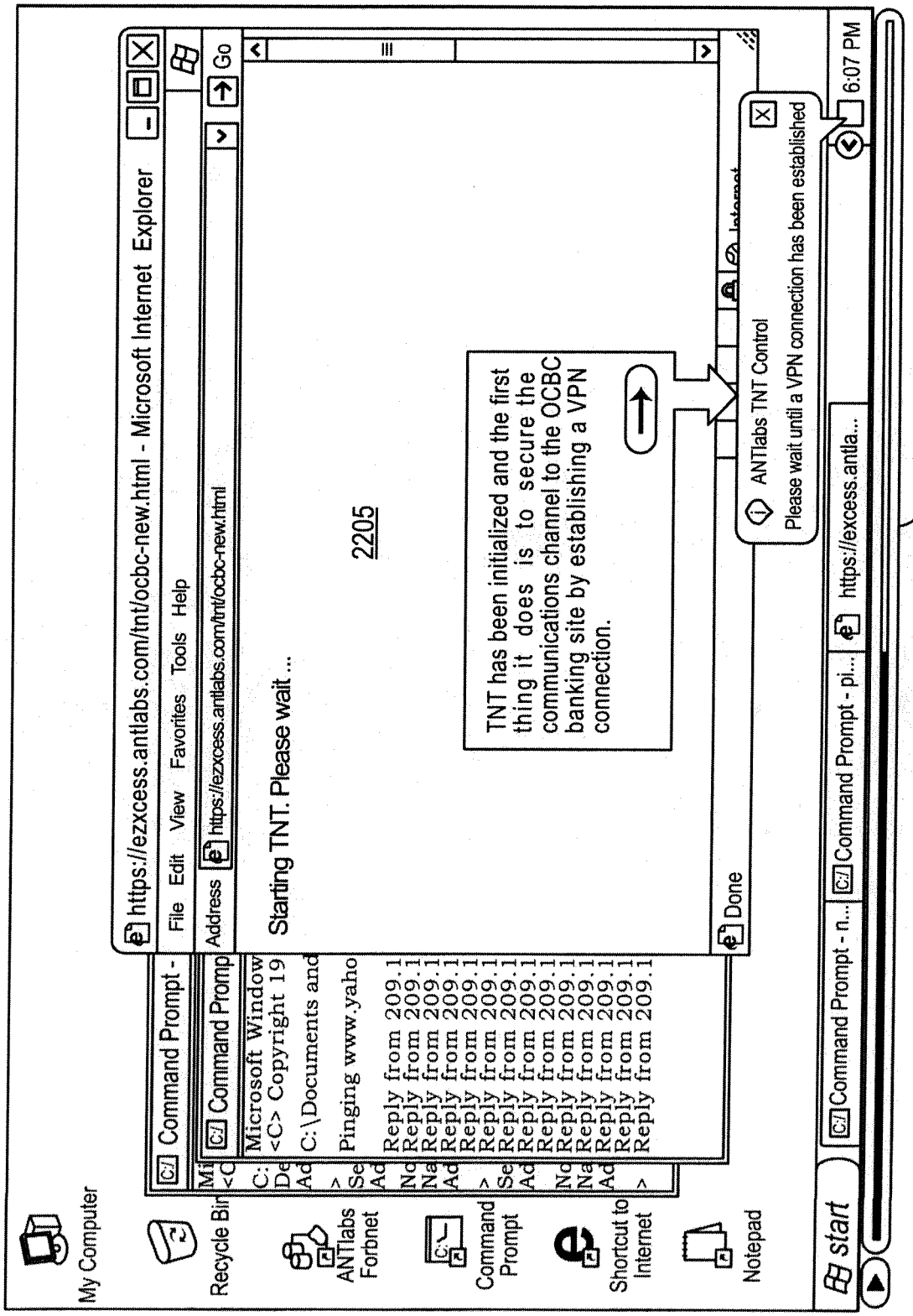

My Computer
Recycle Bin
ANTlabs Forbnet
Command Prompt
Shortcut to Internet
Notepad
start
https://ezxcess.antlabs.com/tnt/ocbc-new.html - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://ezxcess.antlabs.com/tnt/ocbc-new.html
Go
Starting TNT. Please wait ...
2205
TNT has been initialized and the first thing it does is to secure the communications channel to the OCBC banking site by establishing a VPN connection.
Done
Internet
ANTlabs TNT Control
Please wait until a VPN connection has been established
Command Prompt - n...
Command Prompt - pi...
https://excess.antla...
6:07 PM
805

FIG. 22

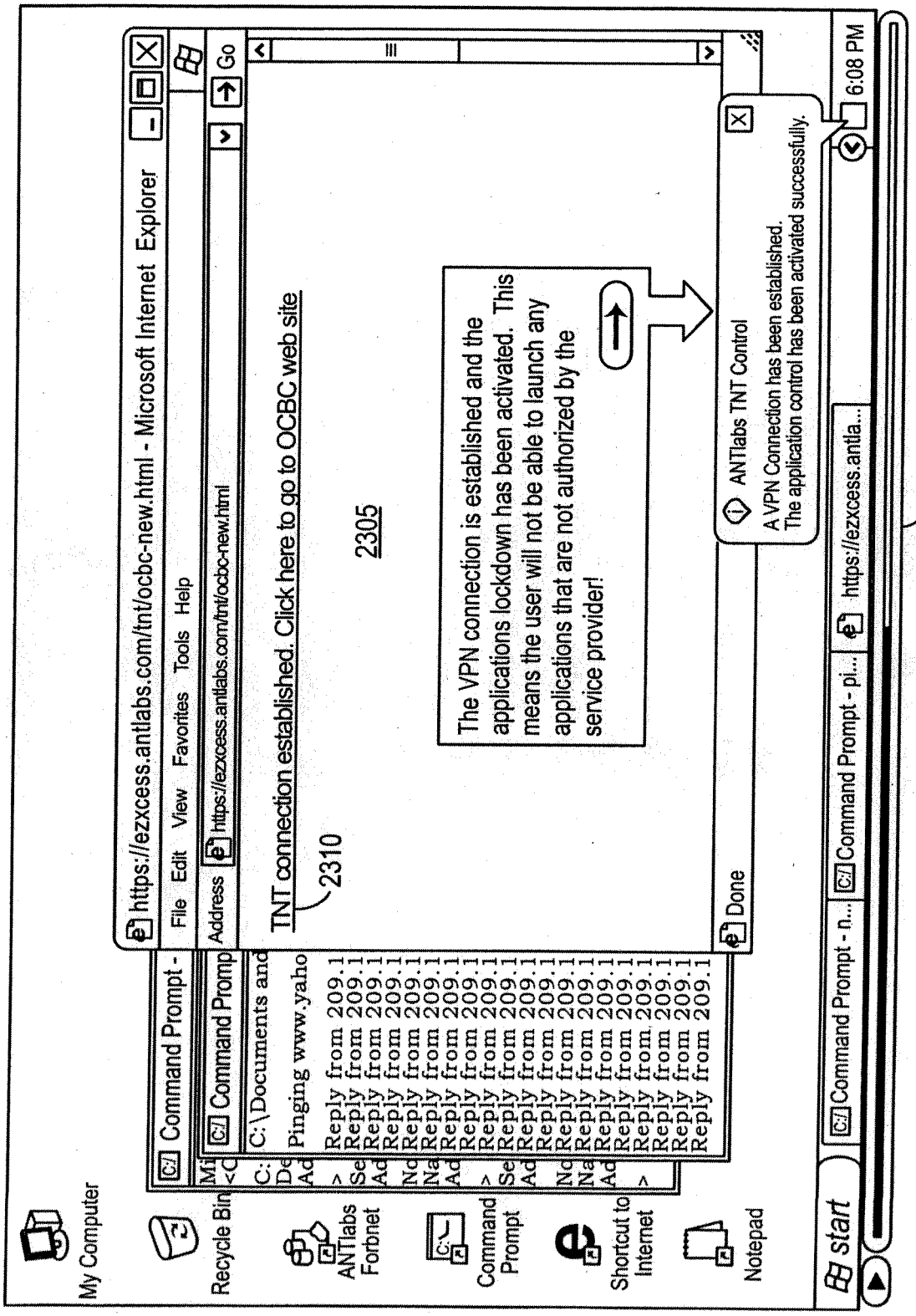

My Computer
Recycle Bin
ANTlabs Forbnet
Command Prompt
Shortcut to Internet
Notepad
https://ezxcess.antlabs.com/tnt/ocbc-new.html - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://ezxcess.antlabs.com/tnt/ocbc-new.html
Go
C:\Documents and
Pinging www.yaho
Reply from 209.1
TNT connection established. Click here to go to OCBC web site
2310
2305
The VPN connection is established and the applications lockdown has been activated. This means the user will not be able to launch any applications that are not authorized by the service provider!
Done
ANTlabs TNT Control
A VPN Connection has been established.
The application control has been activated successfully.
start
Command Prompt - n...
Command Prompt - pi...
https://ezxcess.antla...
6:08 PM
805

FIG. 23

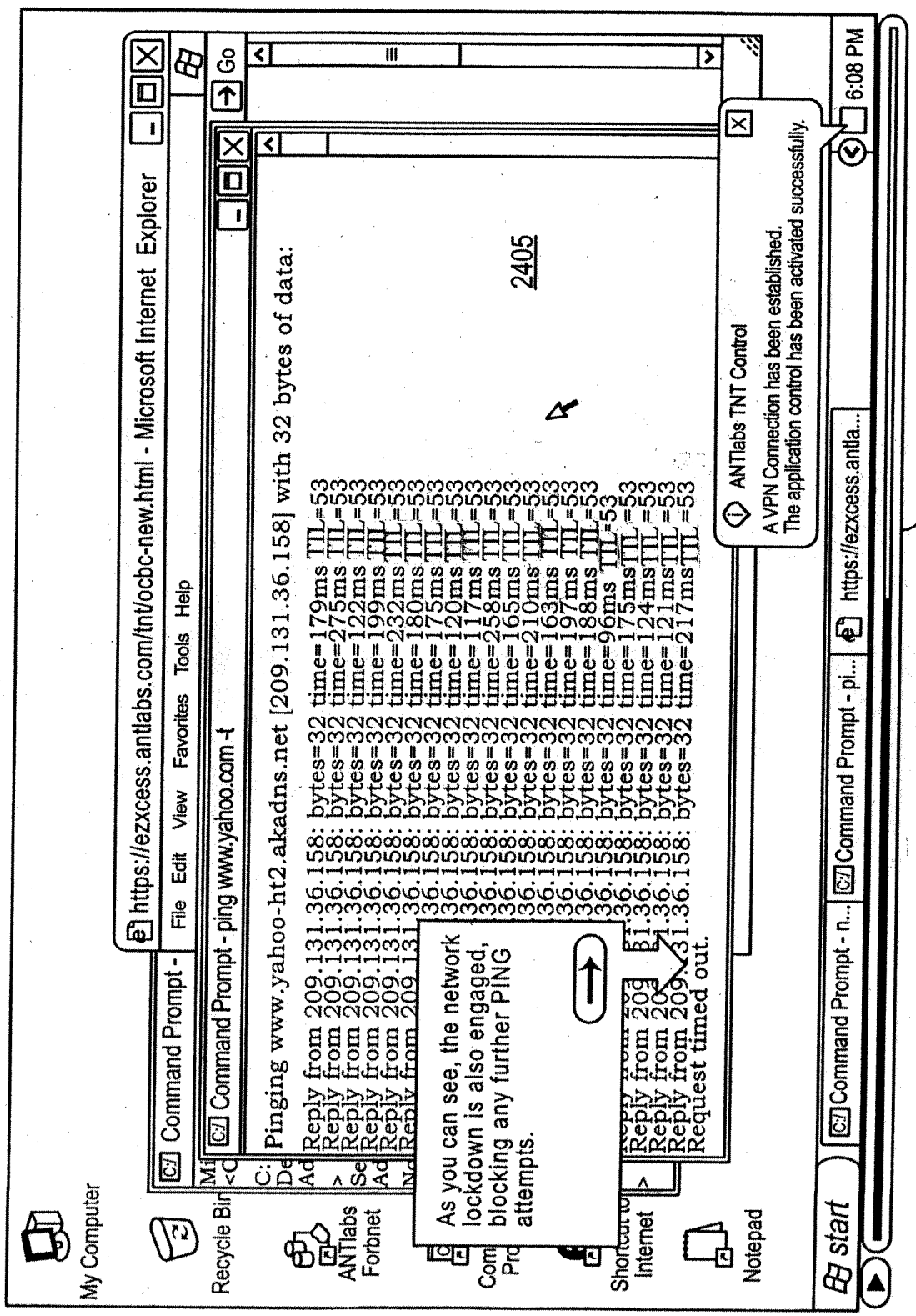

My Computer
Recycle Bin
ANTlabs Forbnet
Internet
Notepad
https://ezxcess.antlabs.com/tnt/ocbc-new.html - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Command Prompt - ping www.yahoo.com -t
Pinging www.yahoo-ht2.akadns.net [209.131.36.158] with 32 bytes of data:
Reply from 209.131.36.158: bytes=32 time=179ms TTL=53
Reply from 209.131.36.158: bytes=32 time=275ms TTL=53
Reply from 209.131.36.158: bytes=32 time=122ms TTL=53
Reply from 209.131.36.158: bytes=32 time=199ms TTL=53
Reply from 209.131.36.158: bytes=32 time=232ms TTL=53
Reply from 209.131.36.158: bytes=32 time=180ms TTL=53
Reply from 209.131.36.158: bytes=32 time=175ms TTL=53
Reply from 209.131.36.158: bytes=32 time=120ms TTL=53
Reply from 209.131.36.158: bytes=32 time=117ms TTL=53
Reply from 209.131.36.158: bytes=32 time=258ms TTL=53
Reply from 209.131.36.158: bytes=32 time=165ms TTL=53
Reply from 209.131.36.158: bytes=32 time=210ms TTL=53
Reply from 209.131.36.158: bytes=32 time=163ms TTL=53
Reply from 209.131.36.158: bytes=32 time=197ms TTL=53
Reply from 209.131.36.158: bytes=32 time=188ms TTL=53
Reply from 209.131.36.158: bytes=32 time=96ms TTL=53
Reply from 209.131.36.158: bytes=32 time=175ms TTL=53
Reply from 209.131.36.158: bytes=32 time=124ms TTL=53
Reply from 209.131.36.158: bytes=32 time=121ms TTL=53
Reply from 209.131.36.158: bytes=32 time=217ms TTL=53
Request timed out.
2405
As you can see, the network lockdown is also engaged, blocking any further PING attempts.
ANTlabs TNT Control
A VPN Connection has been established.
The application control has been activated successfully.
start
Command Prompt - n...
Command Prompt - pi...
https://ezxcess.antla...
6:08 PM
805

FIG. 24

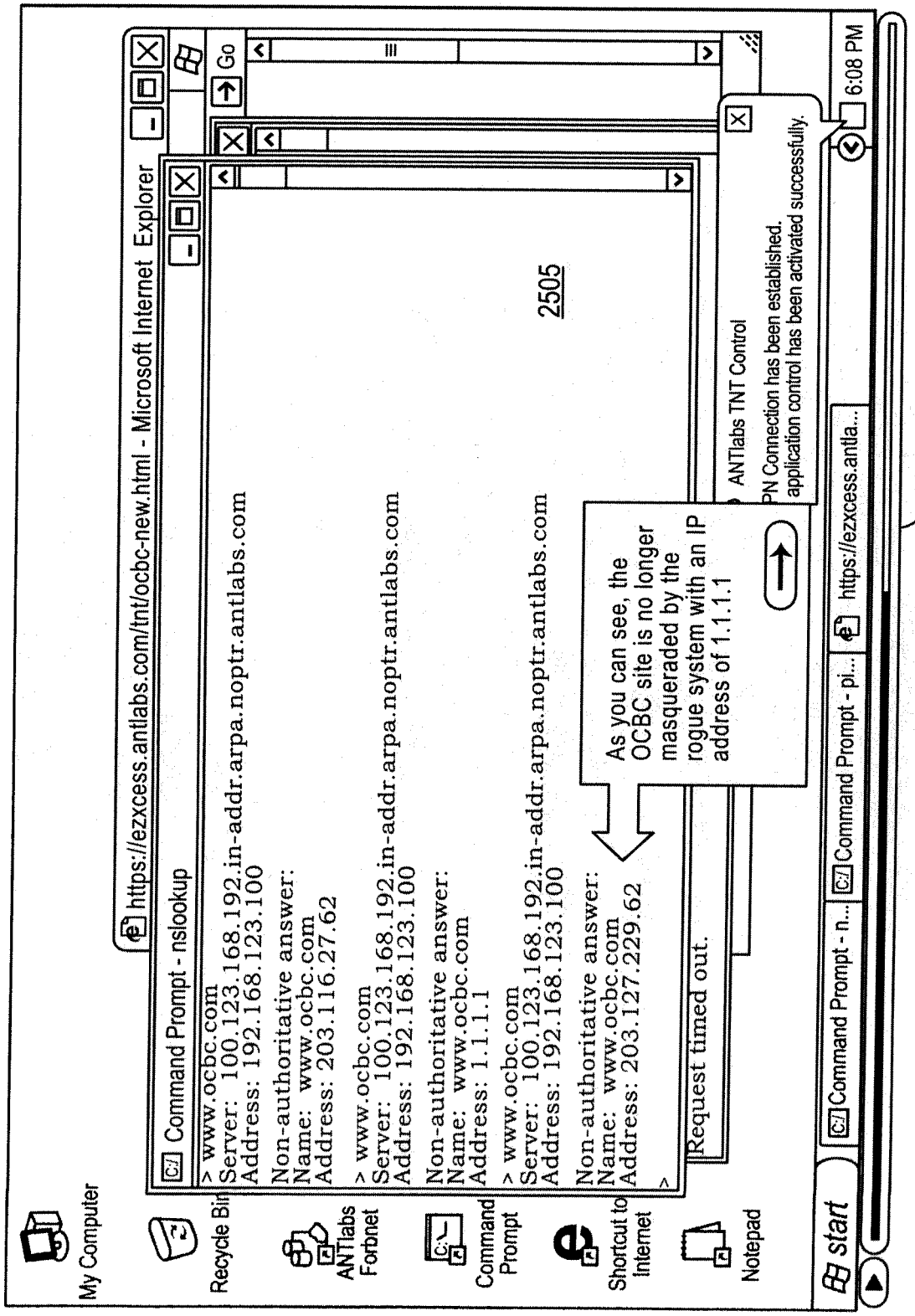

My Computer
Recycle Bin
ANTlabs Forbnet
Command Prompt
Shortcut to Internet
Notepad
https://ezxcess.antlabs.com/tnt/ocbc-new.html - Microsoft Internet Explorer
Command Prompt - nslookup
> www.ocbc.com
Server: 100.123.168.192.in-addr.arpa.noptr.antlabs.com
Address: 192.168.123.100
Non-authoritative answer:
Name: www.ocbc.com
Address: 203.116.27.62
> www.ocbc.com
Server: 100.123.168.192.in-addr.arpa.noptr.antlabs.com
Address: 192.168.123.100
Non-authoritative answer:
Name: www.ocbc.com
Address: 1.1.1.1
> www.ocbc.com
Server: 100.123.168.192.in-addr.arpa.noptr.antlabs.com
Address: 192.168.123.100
Non-authoritative answer:
Name: www.ocbc.com
Address: 203.127.229.62
>
2505
Request timed out.
As you can see, the OCBC site is no longer masqueraded by the rogue system with an IP address of 1.1.1.1
ANTlabs TNT Control
PN Connection has been established.
application control has been activated successfully.
Go
start
Command Prompt - n...
Command Prompt - pi...
https://ezxcess.antla...
6:08 PM
805

FIG. 25

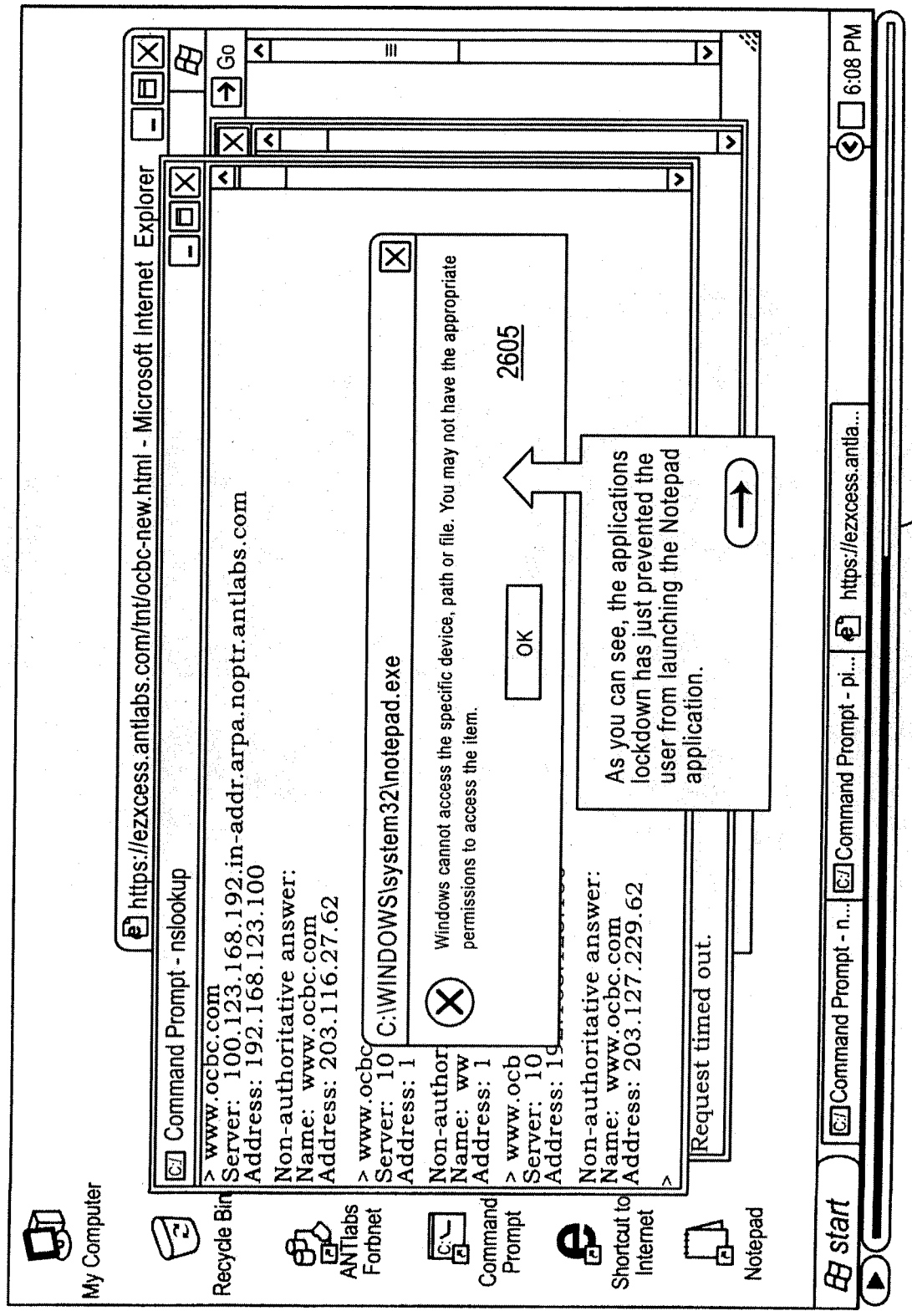

My Computer
Recycle Bin
ANTlabs Forbnet
Command Prompt
Shortcut to Internet
Notepad
https://ezxcess.antlabs.com/tnt/ocbc-new.html - Microsoft Internet Explorer
Command Prompt - nslookup
> www.ocbc.com
Server: 100.123.168.192.in-addr.arpa.noptr.antlabs.com
Address: 192.168.123.100
Non-authoritative answer:
Name: www.ocbc.com
Address: 203.116.27.62
> www.ocbc
Server: 10
Address: 1
Non-author
Name: ww
Address: 1
> www.ocb
Server: 10
Address: 19
Non-authoritative answer:
Name: www.ocbc.com
Address: 203.127.229.62
>
C:\WINDOWS\system32\notepad.exe
Windows cannot access the specific device, path or file. You may not have the appropriate permissions to access the item.
OK
2605
Request timed out.
As you can see, the applications lockdown has just prevented the user from launching the Notepad application.
Go
start
Command Prompt - n...
Command Prompt - pi...
https://ezxcess.antla...
6:08 PM
805

FIG. 26

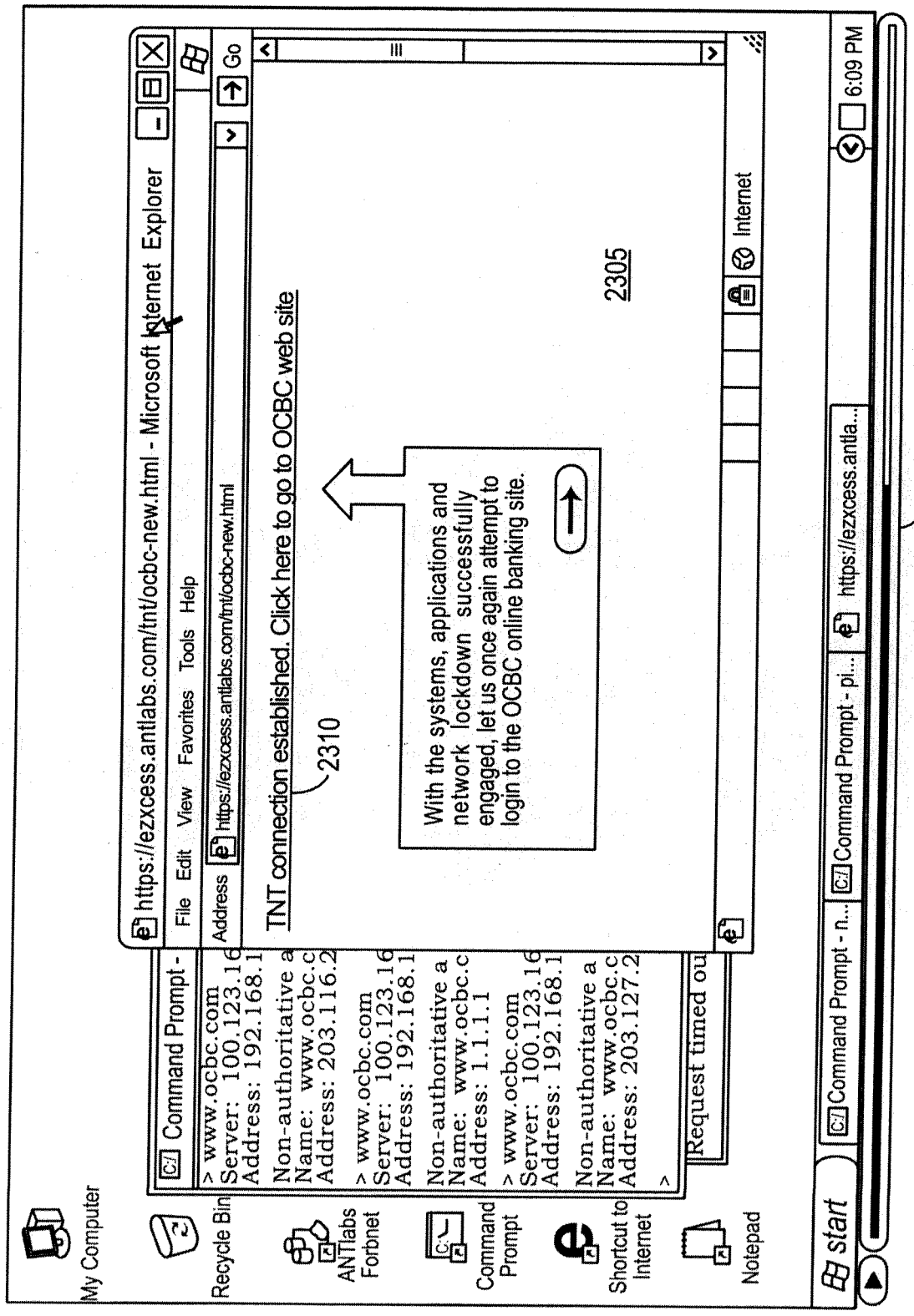

My Computer
Recycle Bin
ANTlabs Forbnet
Command Prompt
Shortcut to Internet
Notepad
https://ezxcess.antlabs.com/tnt/ocbc-new.html - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://ezxcess.antlabs.com/tnt/ocbc-new.html
Go
TNT connection established. Click here to go to OCBC web site
2310
With the systems, applications and network lockdown successfully engaged, let us once again attempt to login to the OCBC online banking site.
2305
Command Prompt -
> www.ocbc.com
Server: 100.123.16
Address: 192.168.1
Non-authoritative a
Name: www.ocbc.c
Address: 203.116.2
> www.ocbc.com
Server: 100.123.16
Address: 192.168.1
Non-authoritative a
Name: www.ocbc.c
Address: 1.1.1.1
> www.ocbc.com
Server: 100.123.16
Address: 192.168.1
Non-authoritative a
Name: www.ocbc.c
Address: 203.127.2
>
Request timed ou
Internet
start
Command Prompt - n...
Command Prompt - pi...
https://ezxcess.antla...
6:09 PM
805

FIG. 27

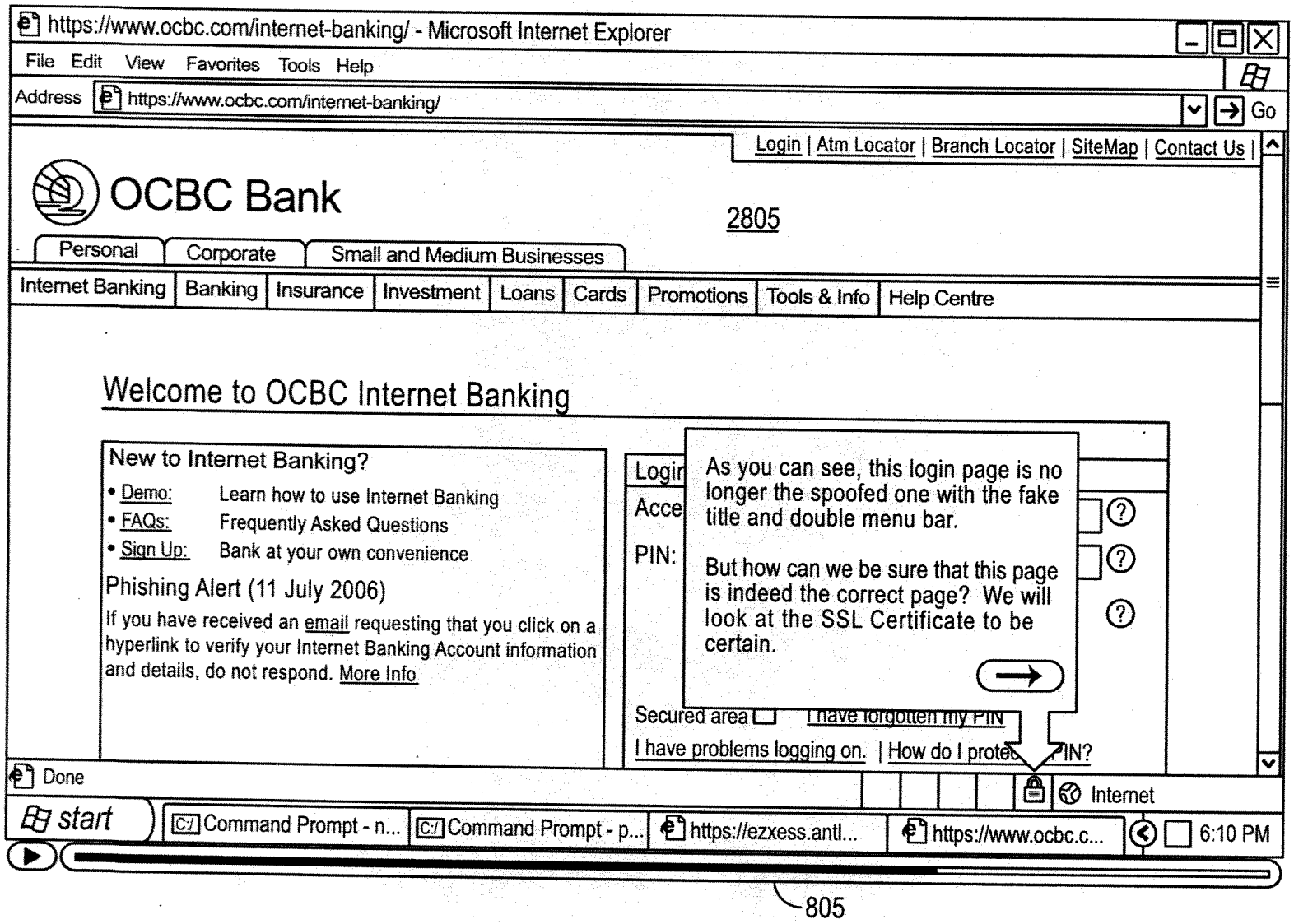

https://www.ocbc.com/internet-banking/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://www.ocbc.com/internet-banking/
Go
Login | Atm Locator | Branch Locator | SiteMap | Contact Us |
OCBC Bank
2805
Personal
Corporate
Small and Medium Businesses
Internet Banking
Banking
Insurance
Investment
Loans
Cards
Promotions
Tools & Info
Help Centre
Welcome to OCBC Internet Banking
New to Internet Banking?
• Demo: Learn how to use Internet Banking
• FAQs: Frequently Asked Questions
• Sign Up: Bank at your own convenience
Phishing Alert (11 July 2006)
If you have received an email requesting that you click on a hyperlink to verify your Internet Banking Account information and details, do not respond. More Info
Login
Acce
PIN:
As you can see, this login page is no longer the spoofed one with the fake title and double menu bar.
But how can we be sure that this page is indeed the correct page? We will look at the SSL Certificate to be certain.
Secured area
I have forgotten my PIN
I have problems logging on.
Done
Internet
start
Command Prompt - n...
Command Prompt - p...
https://ezxess.antl...
https://www.ocbc.c...
6:10 PM
805

FIG. 28

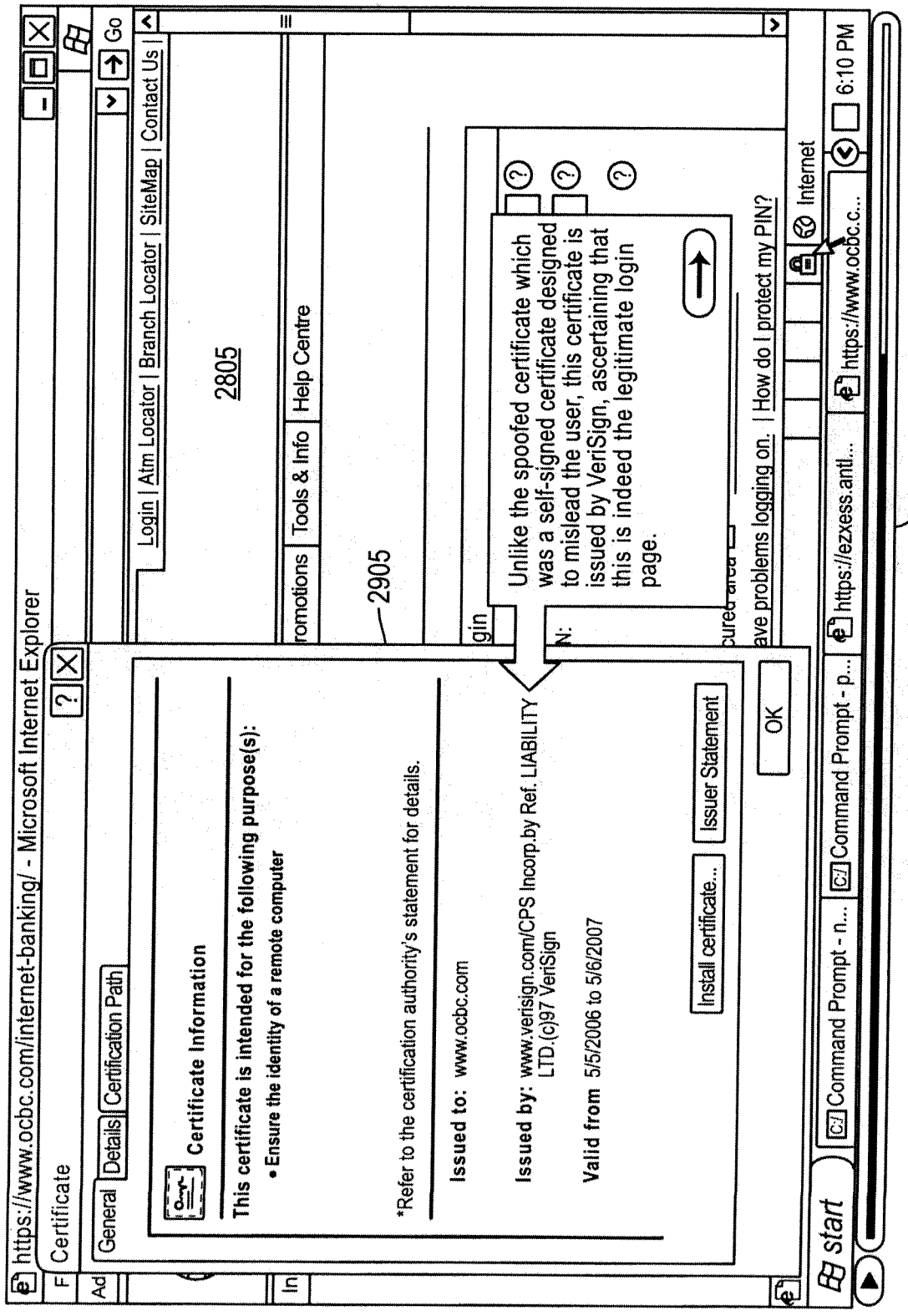

https://www.ocbc.com/internet-banking/ - Microsoft Internet Explorer
Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensure the identity of a remote computer
*Refer to the certification authority's statement for details.
Issued to: www.ocbc.com
Issued by: www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign
Valid from 5/5/2006 to 5/6/2007
Install certificate...
Issuer Statement
OK
Login | Atm Locator | Branch Locator | SiteMap | Contact Us
2805
romotions
Tools & Info
Help Centre
2905
Unlike the spoofed certificate which was a self-signed certificate designed to mislead the user, this certificate is issued by VeriSign, ascertaining that this is indeed the legitimate login page.
ave problems logging on. | How do I protect my PIN?
Internet
start
Command Prompt - n...
Command Prompt - p...
https://ezxess.antl...
https://www.ocbc.c...
6:10 PM
805

FIG. 29

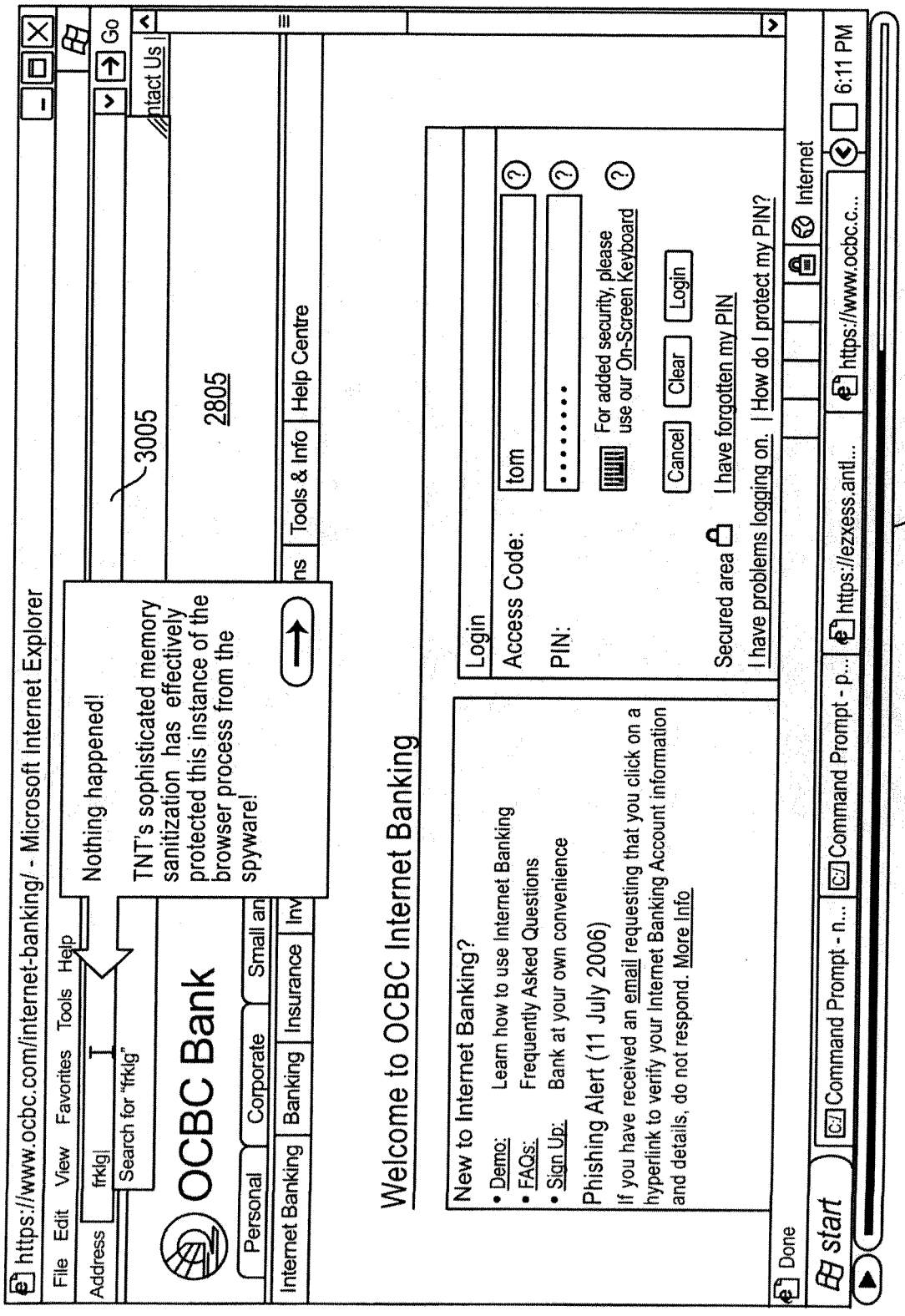

https://www.ocbc.com/internet-banking/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address
Search for "frklg"
Nothing happened!
TNT's sophisticated memory sanitization has effectively protected this instance of the browser process from the spyware!
3005
2805
OCBC Bank
Personal
Corporate
Small an
Internet Banking
Banking
Insurance
Inv
ns
Tools & Info
Help Centre
ntact Us
Welcome to OCBC Internet Banking
New to Internet Banking?
• Demo: Learn how to use Internet Banking
• FAQs: Frequently Asked Questions
• Sign Up: Bank at your own convenience
Phishing Alert (11 July 2006)
If you have received an email requesting that you click on a hyperlink to verify your Internet Banking Account information and details, do not respond. More Info
Login
Access Code:
tom
PIN:
For added security, please use our On-Screen Keyboard
Cancel
Clear
Login
Secured area
I have forgotten my PIN
I have problems logging on. | How do I protect my PIN?
Done
Internet
start
Command Prompt - n...
Command Prompt - p...
https://ezxess.antl...
https://www.ocbc.c...
6:11 PM
805

FIG. 30

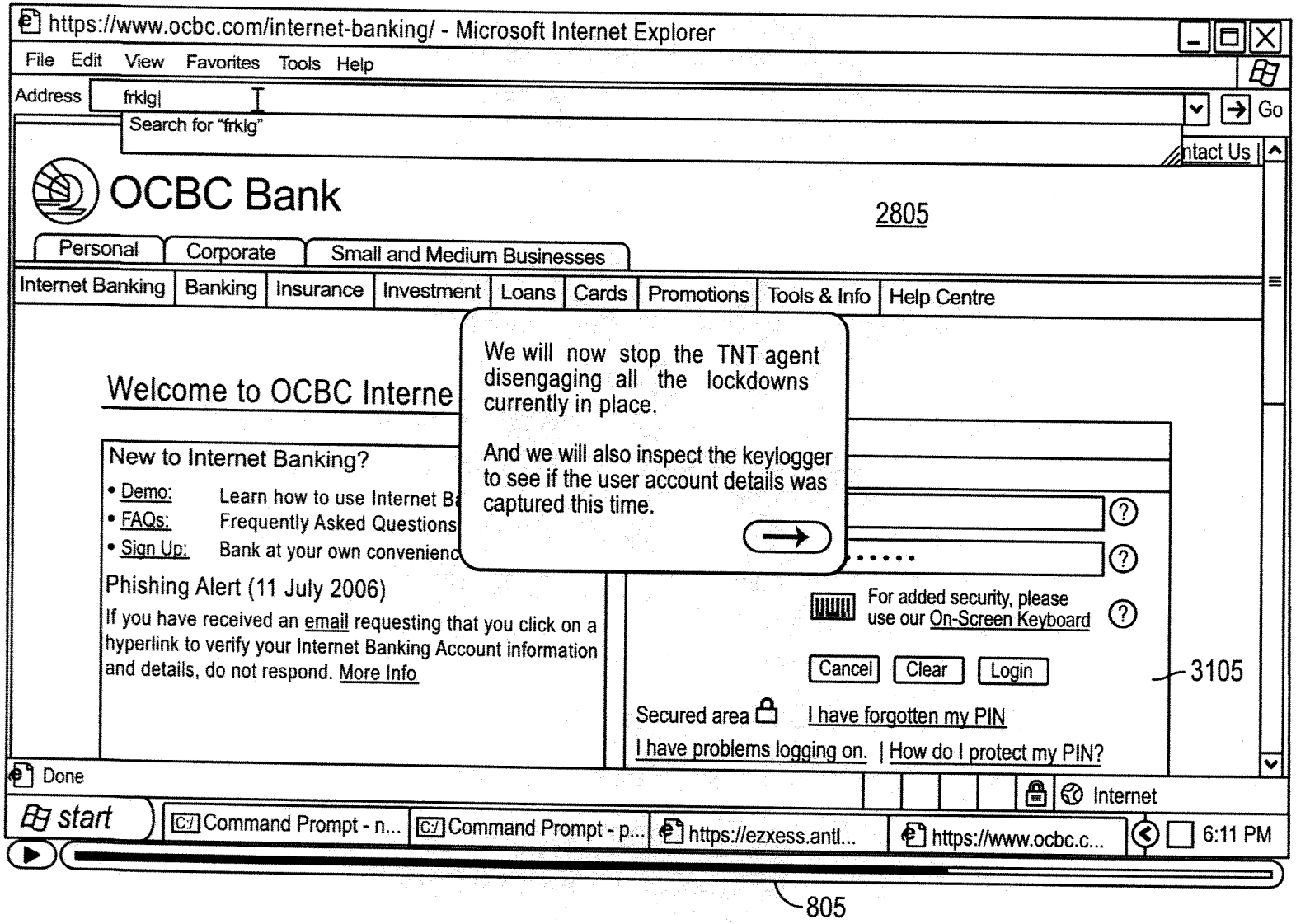

https://www.ocbc.com/internet-banking/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address frklg
Search for "frklg"
Go
ntact Us
OCBC Bank
2805
Personal
Corporate
Small and Medium Businesses
Internet Banking
Banking
Insurance
Investment
Loans
Cards
Promotions
Tools & Info
Help Centre
We will now stop the TNT agent disengaging all the lockdowns currently in place.
And we will also inspect the keylogger to see if the user account details was captured this time.
Welcome to OCBC Interne
New to Internet Banking?
• Demo: Learn how to use Internet Ba
• FAQs: Frequently Asked Questions
• Sign Up: Bank at your own convenienc
Phishing Alert (11 July 2006)
If you have received an email requesting that you click on a hyperlink to verify your Internet Banking Account information and details, do not respond. More Info
For added security, please use our On-Screen Keyboard
Cancel
Clear
Login
3105
Secured area
I have forgotten my PIN
I have problems logging on.
How do I protect my PIN?
Done
Internet
start
Command Prompt - n...
Command Prompt - p...
https://ezxess.antl...
https://www.ocbc.c...
6:11 PM
805

FIG. 31

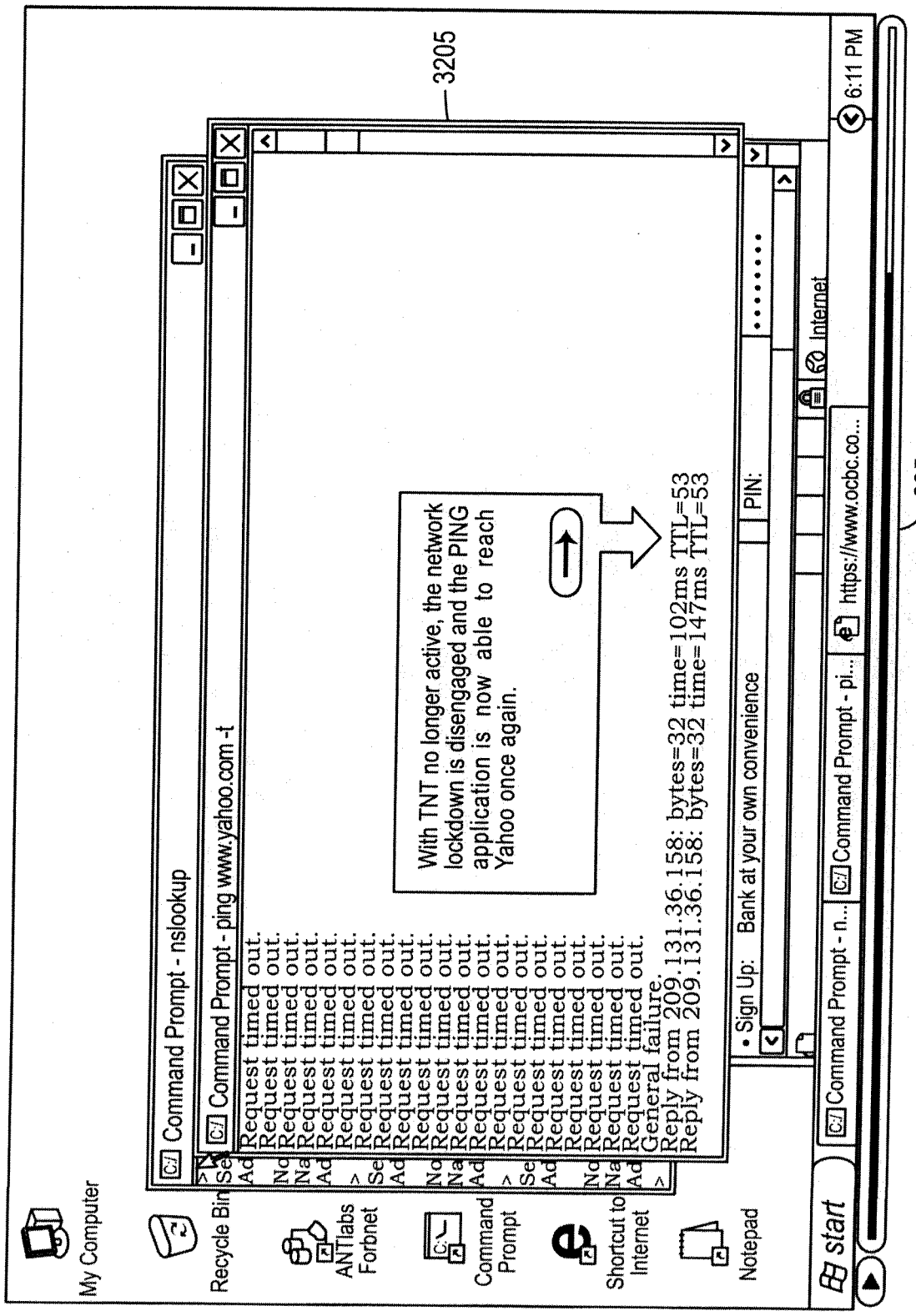

3205
805
Command Prompt - nslookup
Command Prompt - ping www.yahoo.com -t
Request timed out.
Reply from 209.131.36.158: bytes=32 time=102ms TTL=53
Reply from 209.131.36.158: bytes=32 time=147ms TTL=53
General failure.
With TNT no longer active, the network lockdown is disengaged and the PING application is now able to reach Yahoo once again.
• Sign Up: Bank at your own convenience
PIN:
Internet
start
Command Prompt - n...
Command Prompt - pi...
https://www.ocbc.co...
6:11 PM
My Computer
Recycle Bin
ANTlabs Forbnet
Command Prompt
Shortcut to Internet
Notepad

FIG. 32

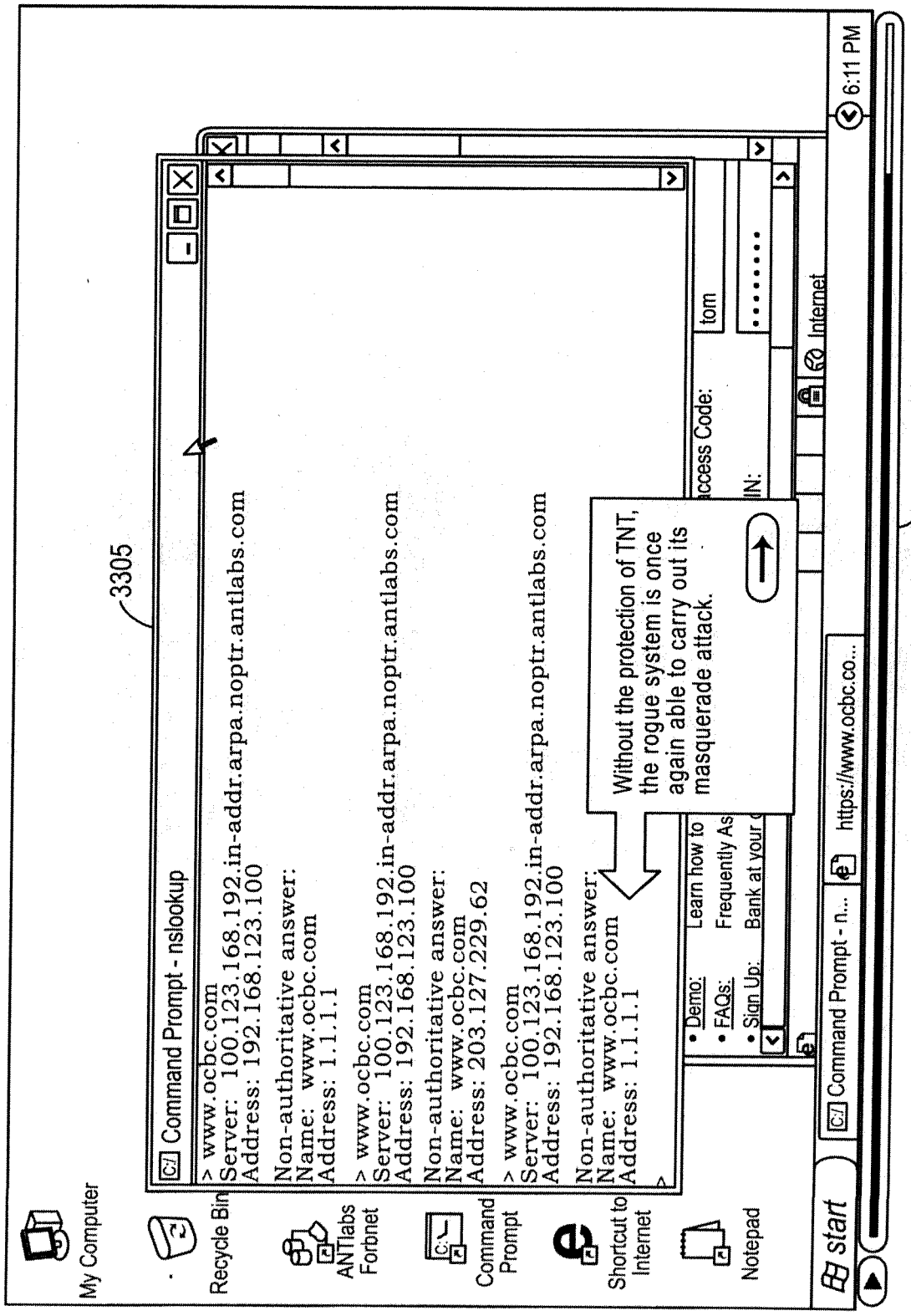

3305
My Computer
Recycle Bin
ANTlabs Forbnet
Command Prompt
Shortcut to Internet
Notepad
Command Prompt - nslookup
> www.ocbc.com
Server: 100.123.168.192.in-addr.arpa.noptr.antlabs.com
Address: 192.168.123.100
Non-authoritative answer:
Name: www.ocbc.com
Address: 1.1.1.1
> www.ocbc.com
Server: 100.123.168.192.in-addr.arpa.noptr.antlabs.com
Address: 192.168.123.100
Non-authoritative answer:
Name: www.ocbc.com
Address: 203.127.229.62
> www.ocbc.com
Server: 100.123.168.192.in-addr.arpa.noptr.antlabs.com
Address: 192.168.123.100
Non-authoritative answer:
Name: www.ocbc.com
Address: 1.1.1.1
Without the protection of TNT, the rogue system is once again able to carry out its masquerade attack.
Demo:
FAQs:
Sign Up:
Learn how to
Frequently As
Bank at your
ccess Code:
tom
IN:
Internet
start
Command Prompt - n...
https://www.ocbc.co...
6:11 PM
805

FIG. 33

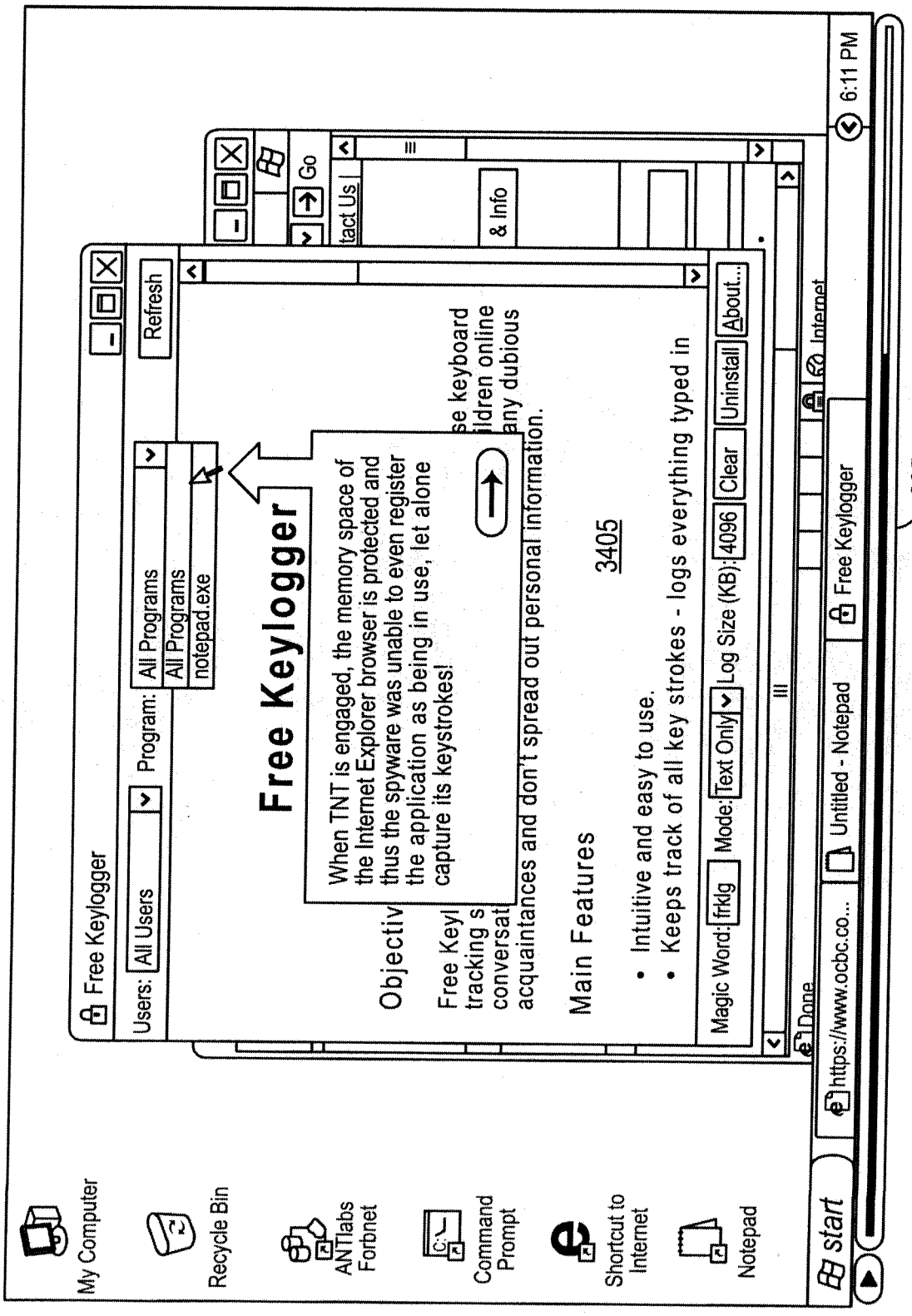

My Computer
Recycle Bin
ANTlabs Forbnet
Command Prompt
Shortcut to Internet
Notepad
start
https://www.ocbc.co...
Untitled - Notepad
Free Keylogger
6:11 PM
805
Free Keylogger
Users: All Users
Program: All Programs
All Programs
notepad.exe
Refresh
Go
tact Us
& Info
When TNT is engaged, the memory space of the Internet Explorer browser is protected and thus the spyware was unable to even register the application as being in use, let alone capture its keystrokes!
Objectiv
Free Keyl
tracking s
conversat
se keyboard
ildren online
any dubious
acquaintances and don't spread out personal information.
Main Features
3405
• Intuitive and easy to use.
• Keeps track of all key strokes - logs everything typed in
Magic Word: frkdg
Mode: Text Only
Log Size (KB): 4096
Clear
Uninstall
About...
Done
Internet

FIG. 34

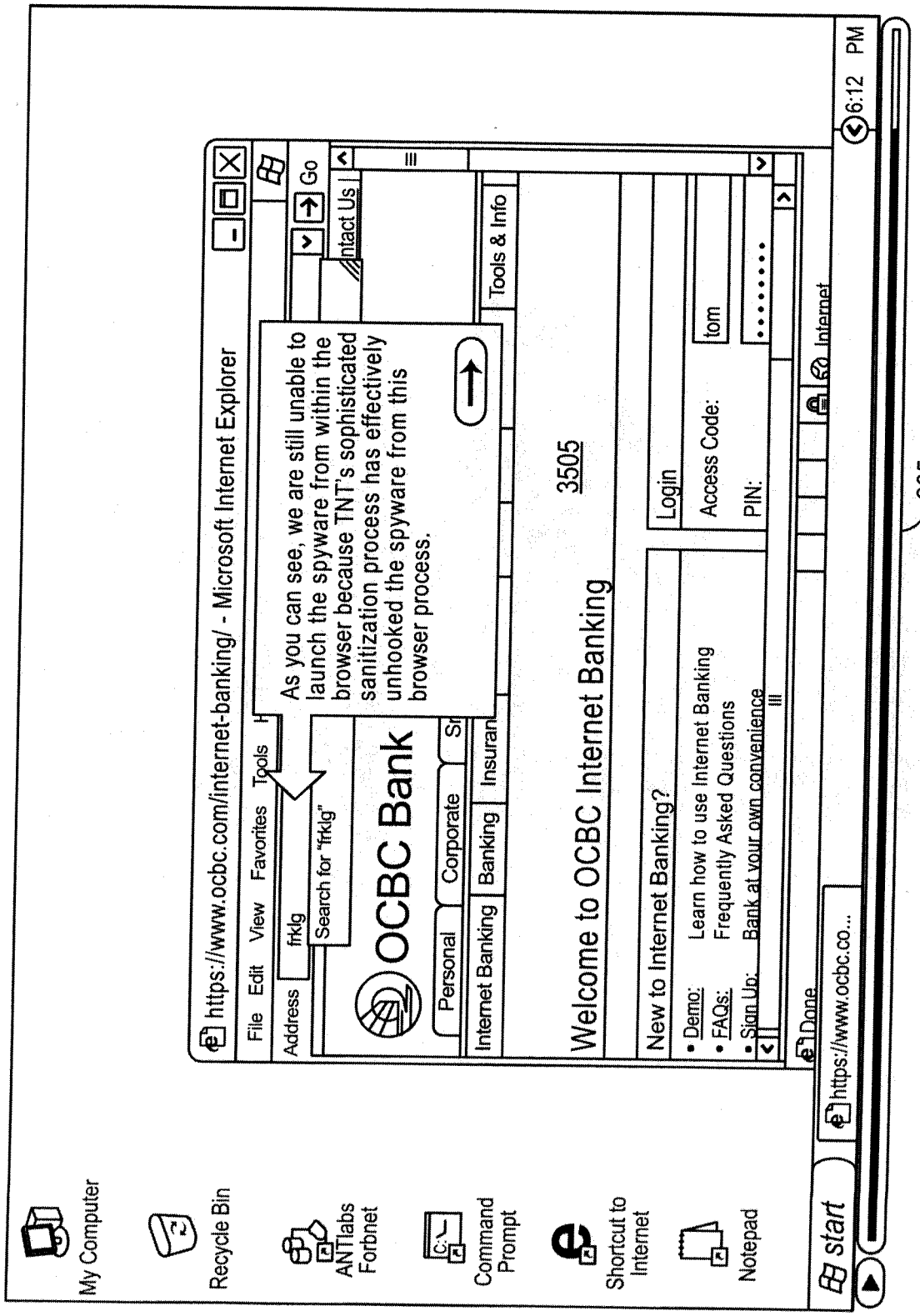

My Computer
Recycle Bin
ANTIabs Forbnet
Command Prompt
Shortcut to Internet
Notepad
start
https://www.ocbc.co...
https://www.ocbc.com/internet-banking/ - Microsoft Internet Explorer
File Edit View Favorites Tools H
Address frklg
Search for "frklg"
As you can see, we are still unable to launch the spyware from within the browser because TNT's sophisticated sanitization process has effectively unhooked the spyware from this browser process.
Go
ntact Us
OCBC Bank
Personal Corporate Sr
Internet Banking Banking Insuran
Tools & Info
Welcome to OCBC Internet Banking
3505
New to Internet Banking?
• Demo: Learn how to use Internet Banking
• FAQs: Frequently Asked Questions
• Sign Up: Bank at your own convenience
Login
Access Code: tom
PIN: •••••••
Done
Internet
6:12 PM
805

FIG. 35