Appendix A

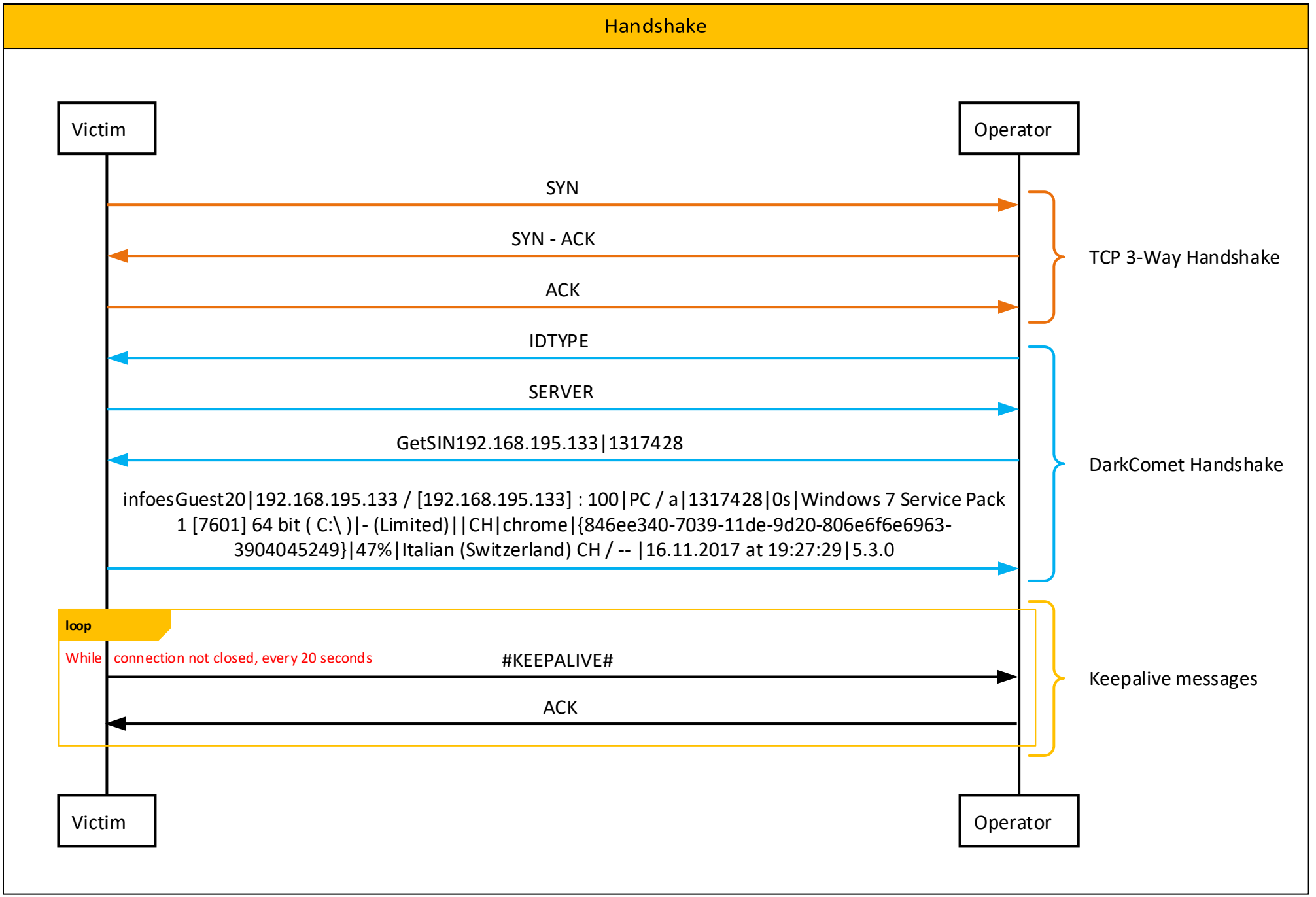
Begin of Darkcomet Commands documentation

Each command has been simulated in a virtual environment, dumped with tcpdump and decrypted with a proper script in order to figure out its behavior.

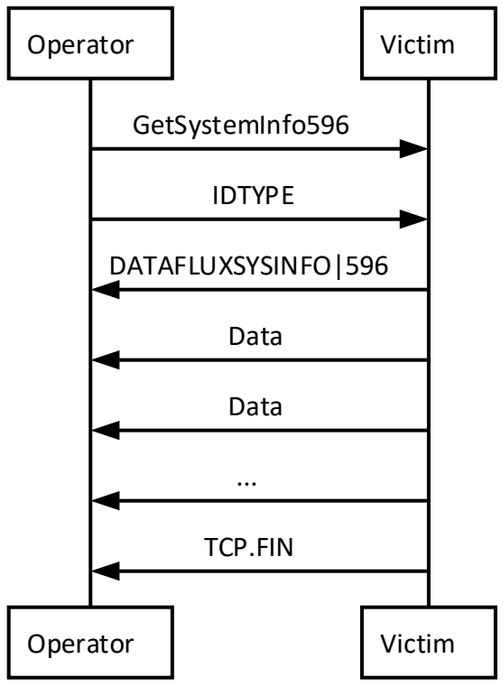
The following diagrams describe all commands doable from the DarkComet Operator side.

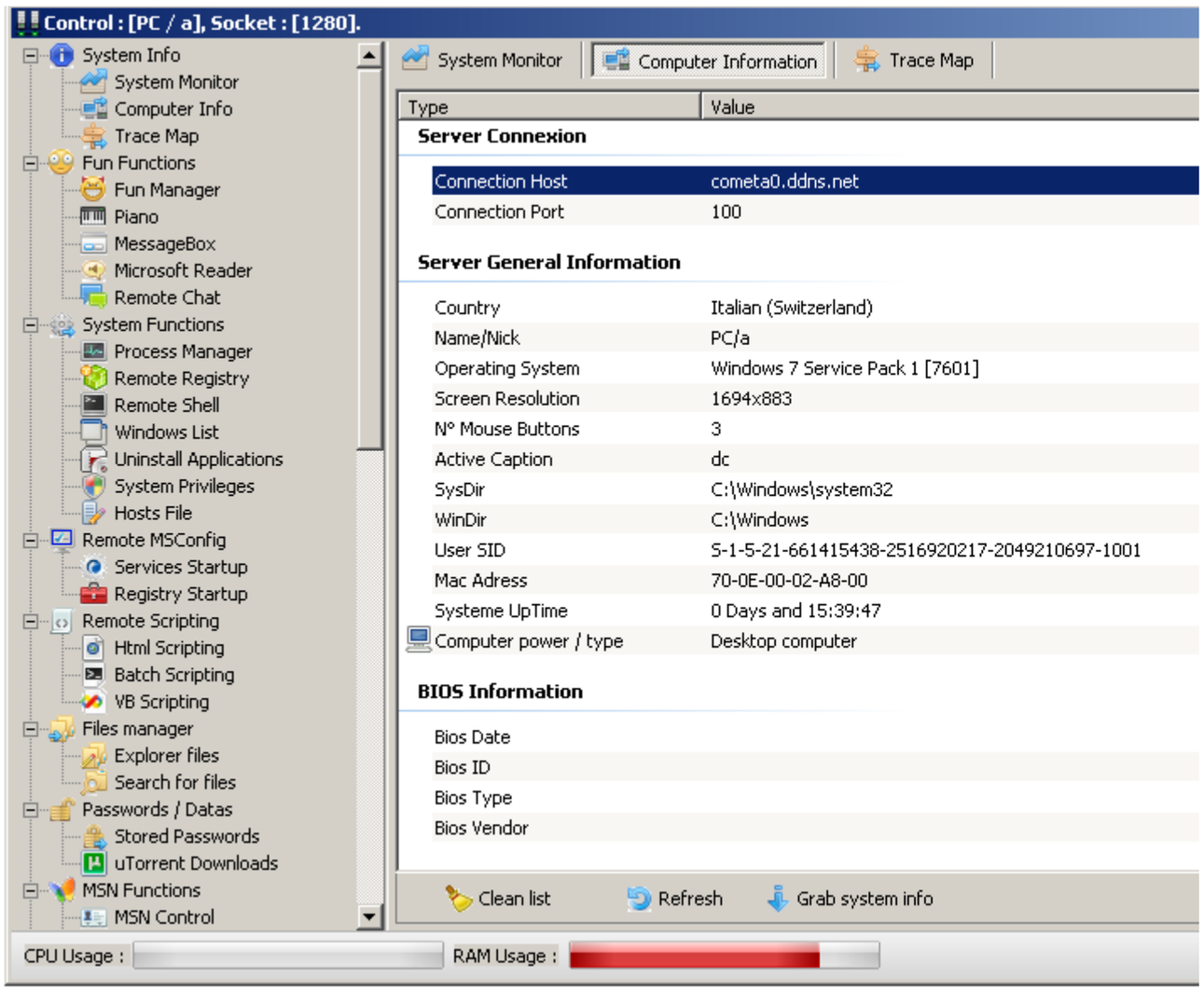
The text right to a data flux, is normally what is the file or the text sent in this data stream. If colours are present, they indicate a difference from the previous/next command.

By Sandro Tiago Carlao (tiags1@bfh.ch)


Handshake
Victim
Operator
SYN
SYN - ACK
ACK
TCP 3-Way Handshake
IDTYPE
SERVER
GetSIN192.168.195.133|1317428
infoesGuest20|192.168.195.133 / [192.168.195.133] : 100|PC / a|1317428|0s|Windows 7 Service Pack 1 [7601] 64 bit (C:\ )|- (Limited)||CH|chrome|{846ee340-7039-11de-9d20-806e6f6e6963-3904045249}|47%|Italian (Switzerland) CH / -- |16.11.2017 at 19:27:29|5.3.0
DarkComet Handshake
loop
While connection not closed, every 20 seconds
#KEEPALIVE#
ACK
Keepalive messages
Victim
Operator

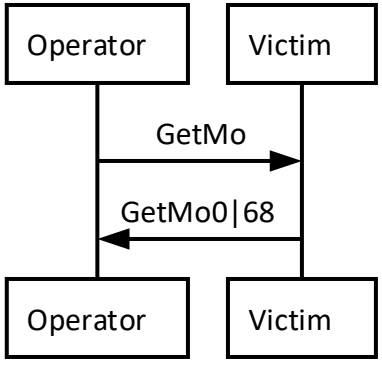
System Info -> System Information

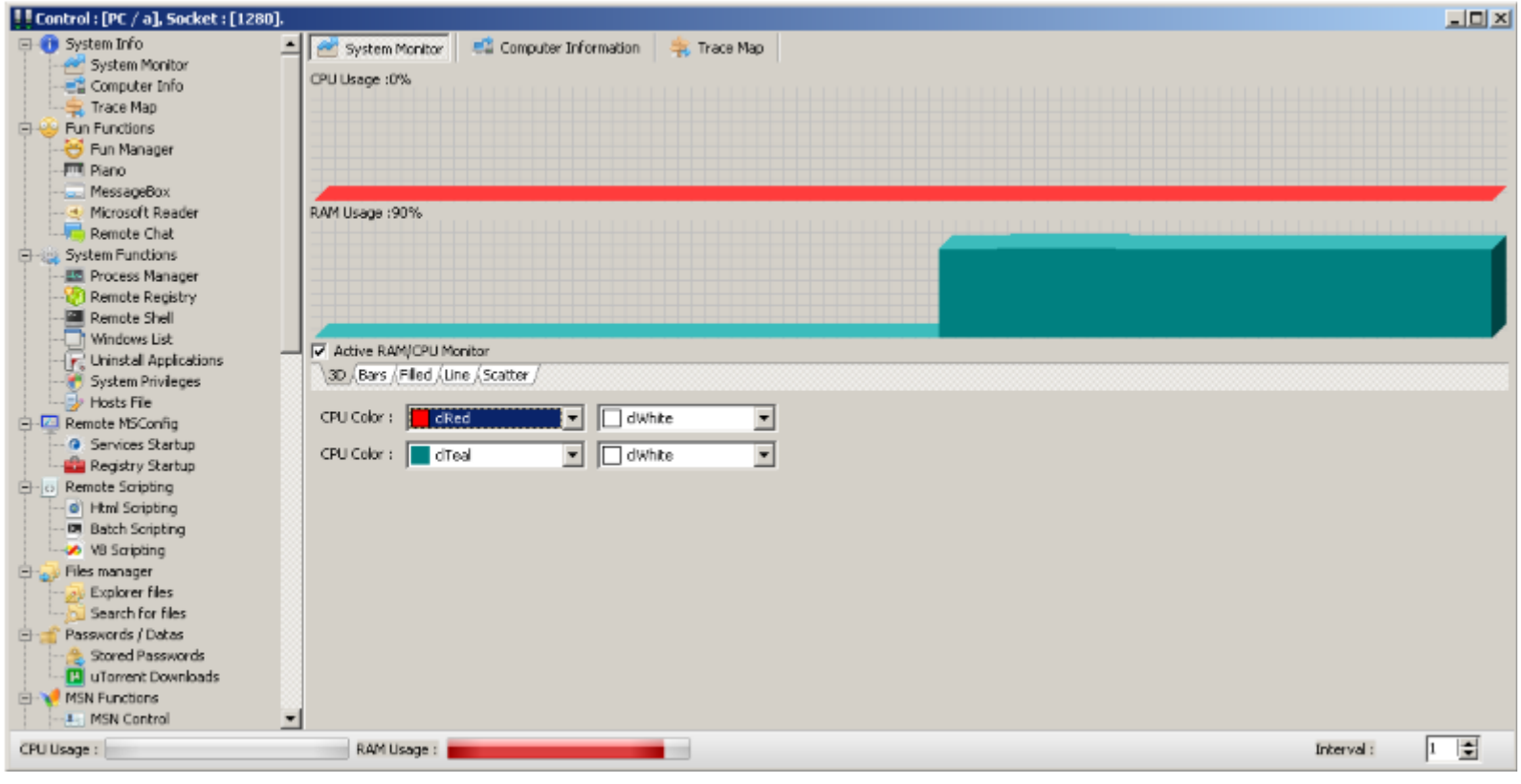




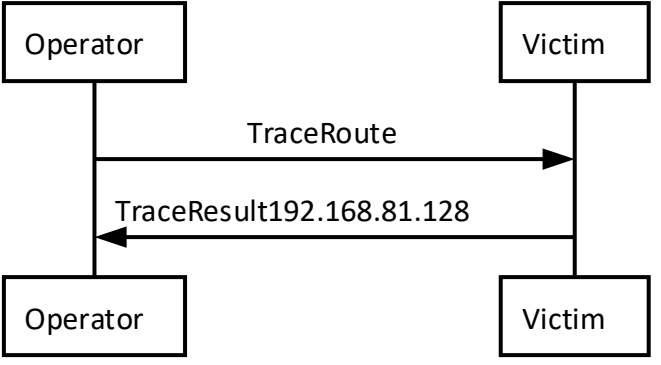
Host Name: PC
OS Name: Microsoft Windows 7 Professional
OS Version: 6.1.7601 Service Pack 1 Build 7601
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Workstation
OS Build Type: Multiprocessor Free
Registered Owner: a
Registered Organization:
Product ID: 00371-177-0000061-85899
Original Install Date: 15.11.2017, 19:07:22
System Boot Time: 16.04.2018, 18:47:00
System Manufacturer: VMware, Inc.
System Model: VMware Virtual Platform
System Type: x64-based PC
Processor(s): 2 Processor(s) Installed.
[01]: Intel64 Family 6 Model 94 Stepping 3 GenuineIntel ~2592 Mhz
[02]: Intel64 Family 6 Model 94 Stepping 3 GenuineIntel ~2592 Mhz
BIOS Version: Phoenix Technologies LTD 6.00, 19.05.2017
Windows Directory: C:\Windows
System Directory: C:\Windows\system32
Boot Device: \Device\HarddiskVolume1
System Locale: it-ch;Italian (Switzerland)
Input Locale: fr-ch;French (Switzerland)
Time Zone: (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
Total Physical Memory: 2'047 MB
Available Physical Memory: 280 MB
Virtual Memory: Max Size: 4'095 MB
Virtual Memory: Available: 797 MB
Virtual Memory: In Use: 3'298 MB
Page File Location(s): C:\pagefile.sys
Domain: WORKGROUP
Logon Server: \\PC
Hotfix(s): 5 Hotfix(s) Installed.
[01]: KB2534111
[02]: KB2882822
[03]: KB2999226
[04]: KB4019990
[05]: KB976902
Network Card(s): 2 NIC(s) Installed.
[01]: Intel(R) PRO/1000 MT Network Connection
Connection Name: Local Area Connection
DHCP Enabled: Yes
DHCP Server: 192.168.81.254
IP address(es)
[01]: 192.168.81.128
[02]: Microsoft Loopback Adapter
Connection Name: Npcap Loopback Adapter
DHCP Enabled: Yes
DHCP Server: 255.255.255.255
IP address(es)
[01]: 169.254.15.224
[02]: fe80::a496:be44:b749:fe0

System Info -> System monitor

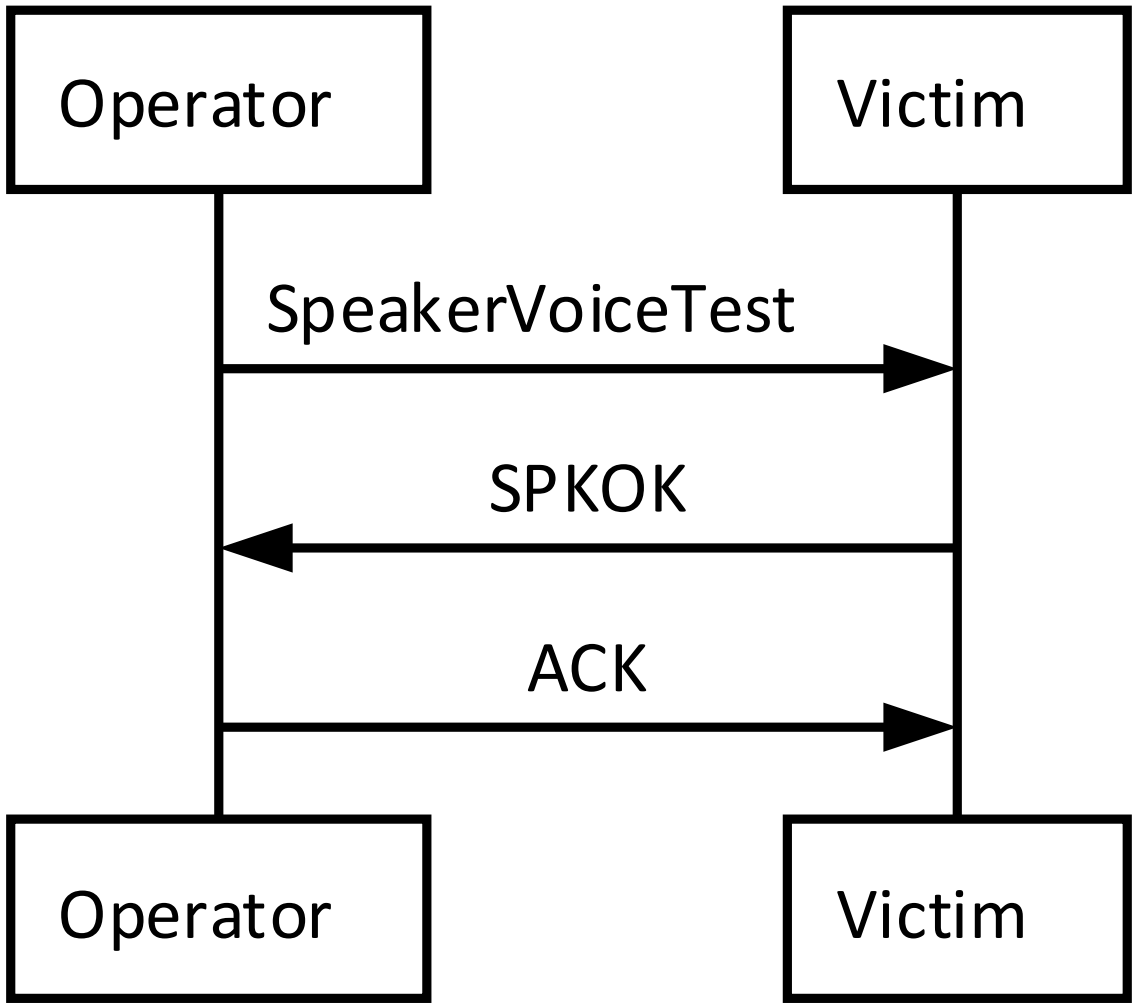




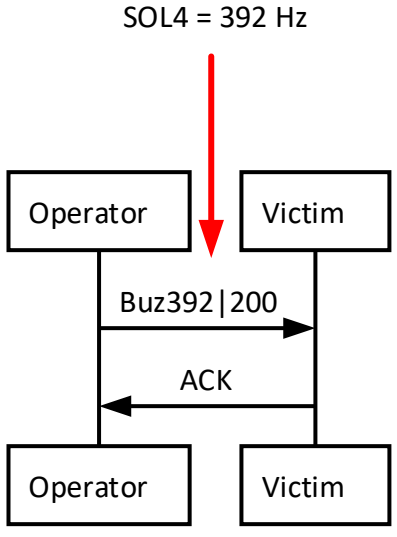
System Info -> Trace Map

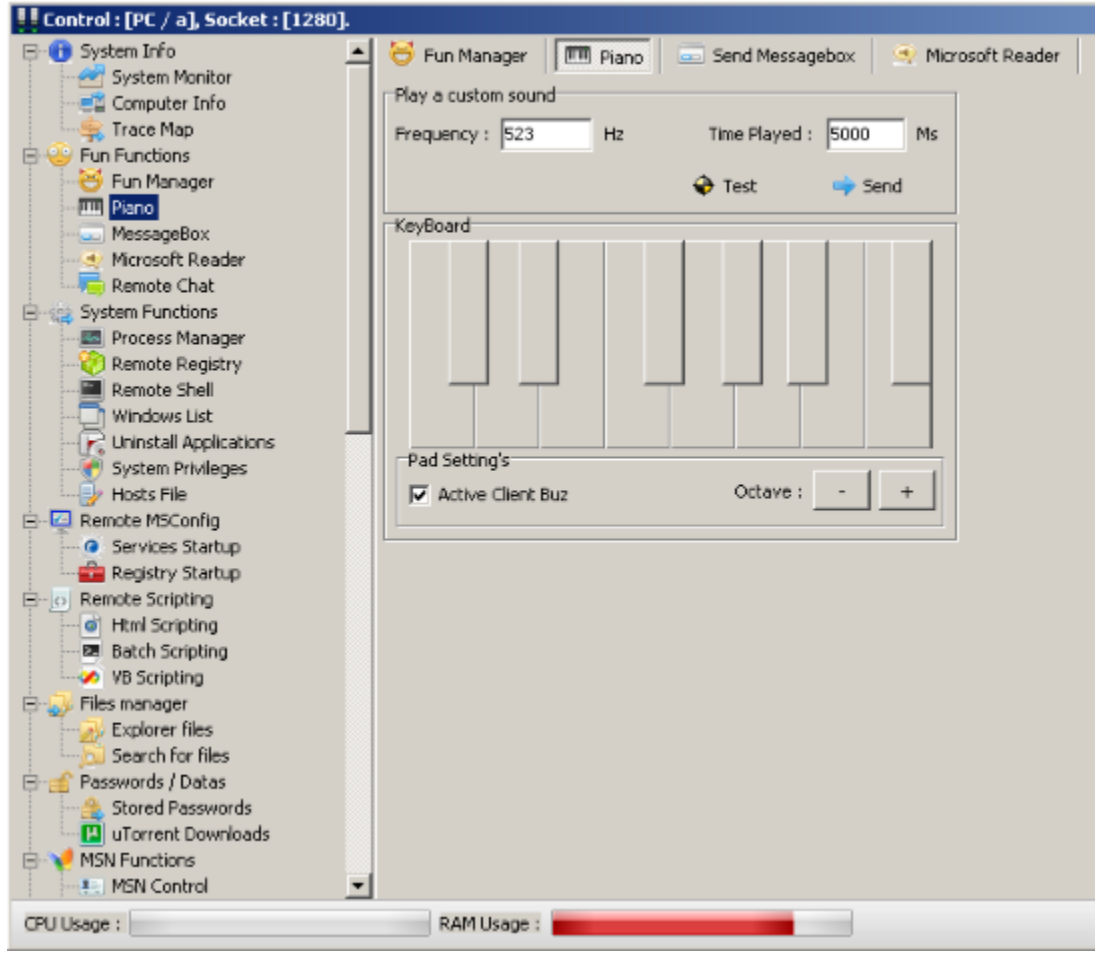


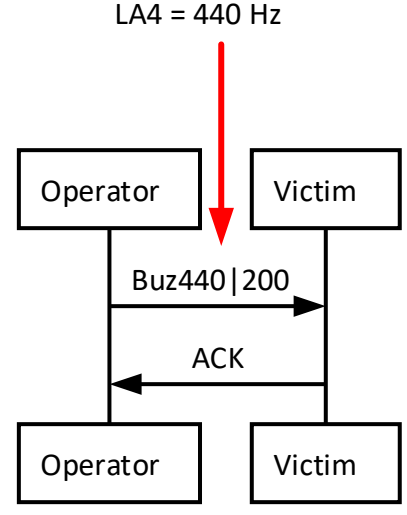
Fun Functions -> Microsoft Reader



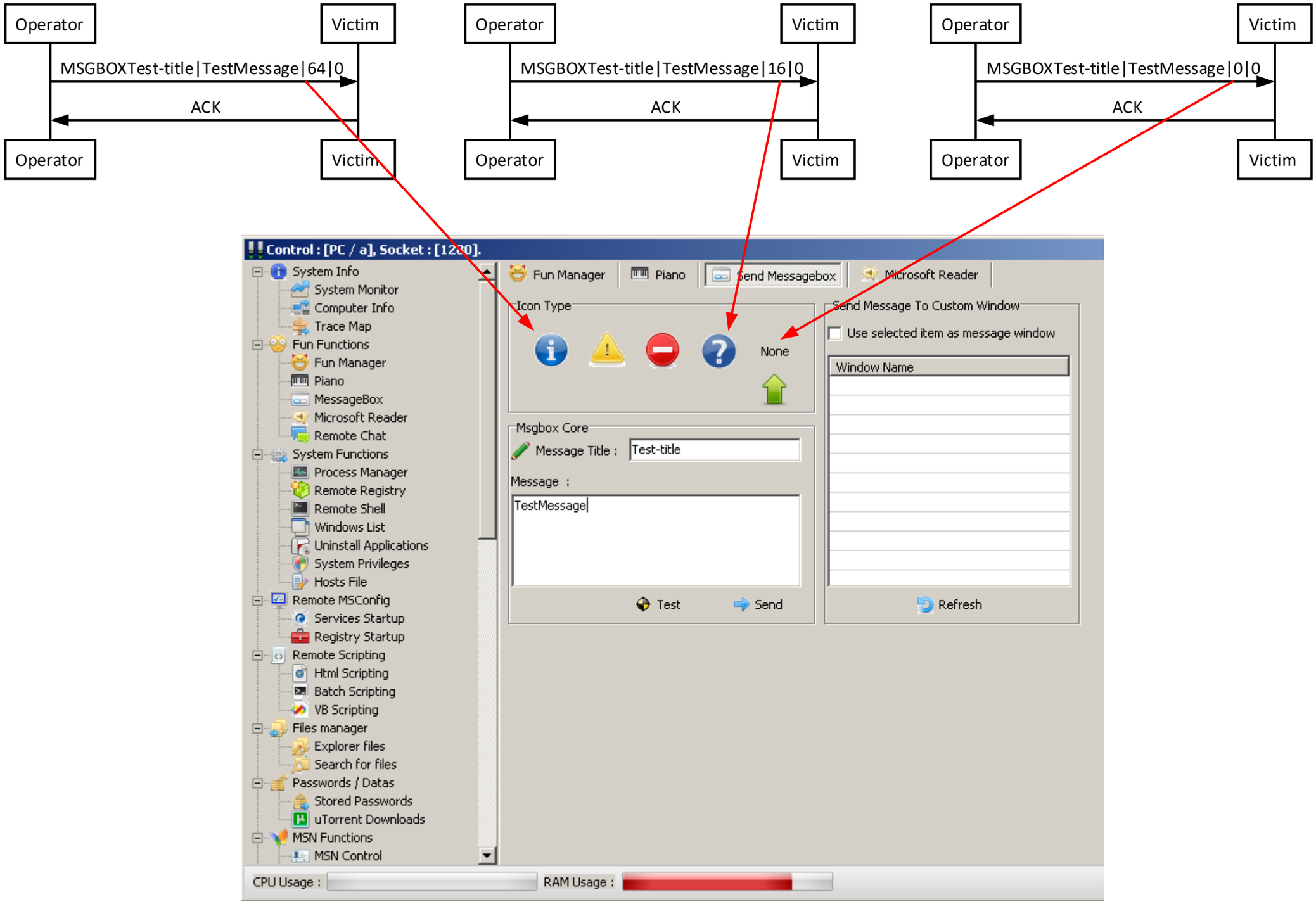
Fun Functions -> Piano



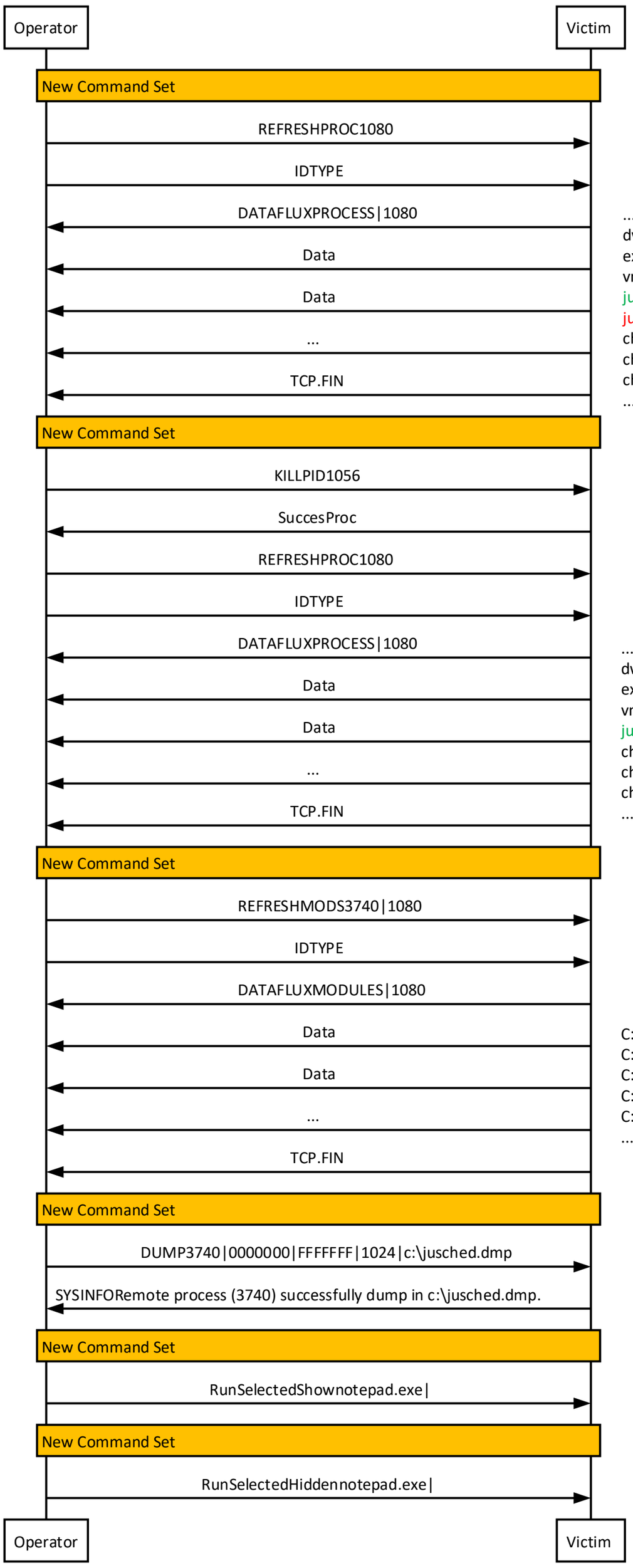




Fun Functions -> Send MessageBox



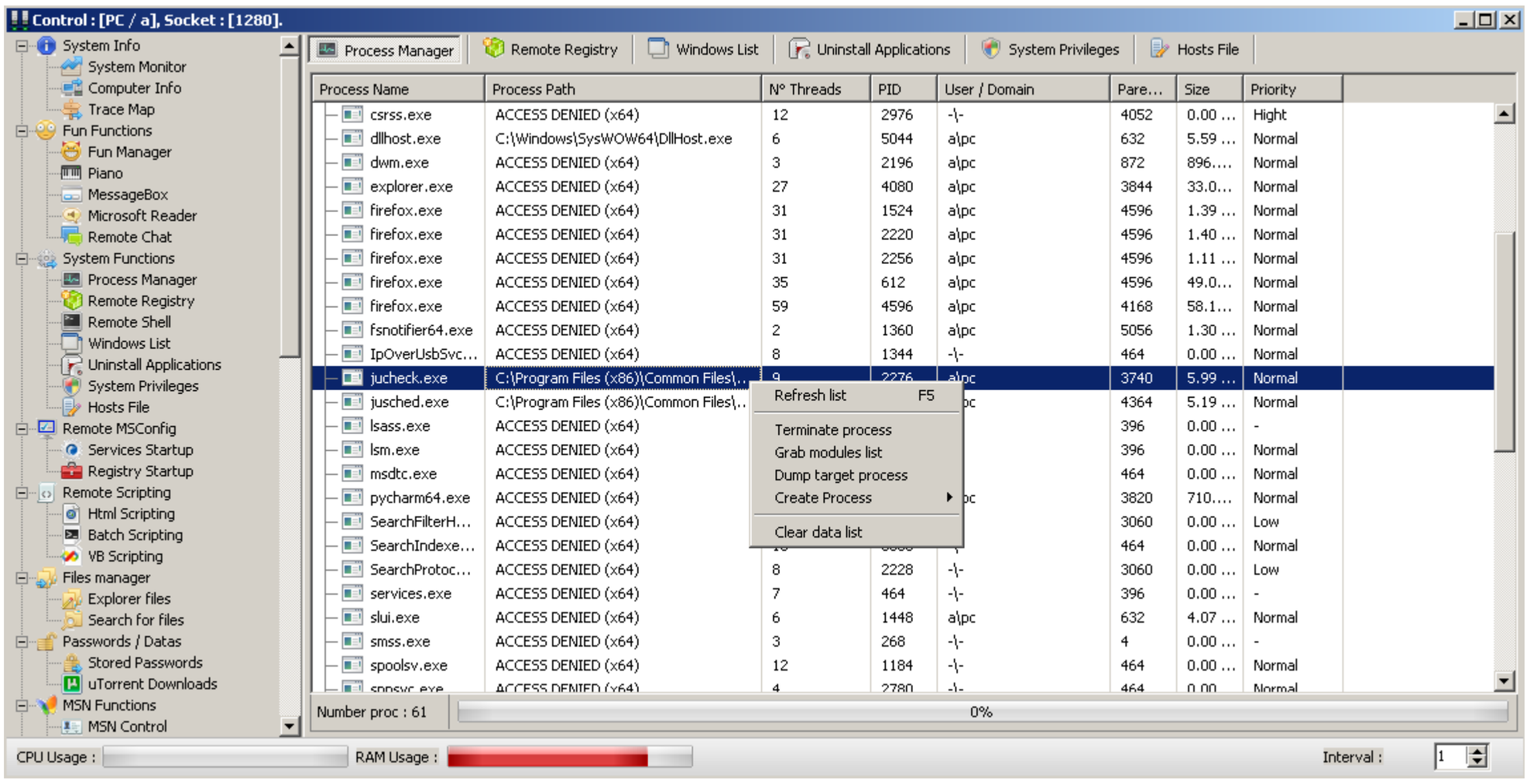
System Functions -> Process Manager

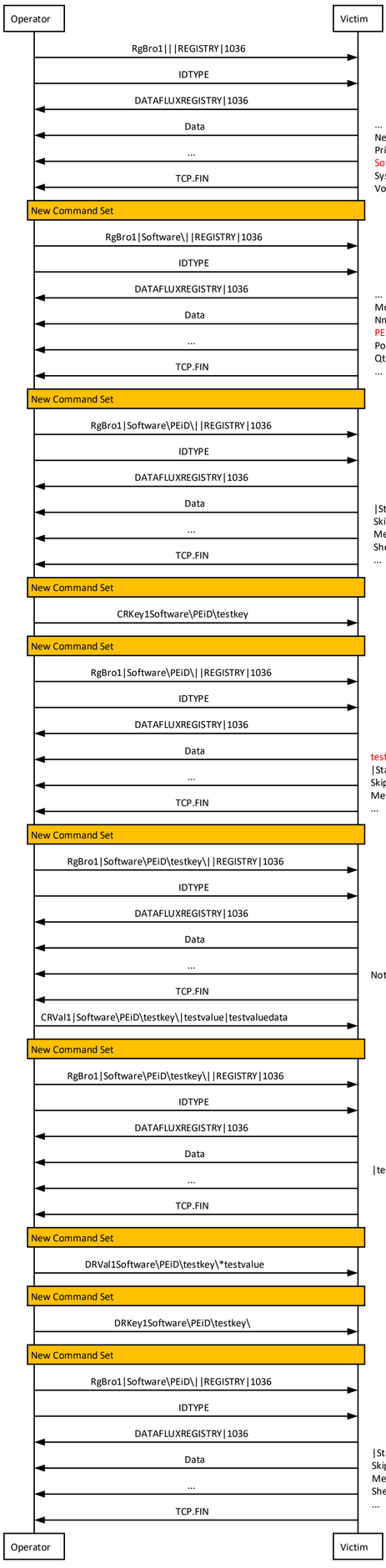


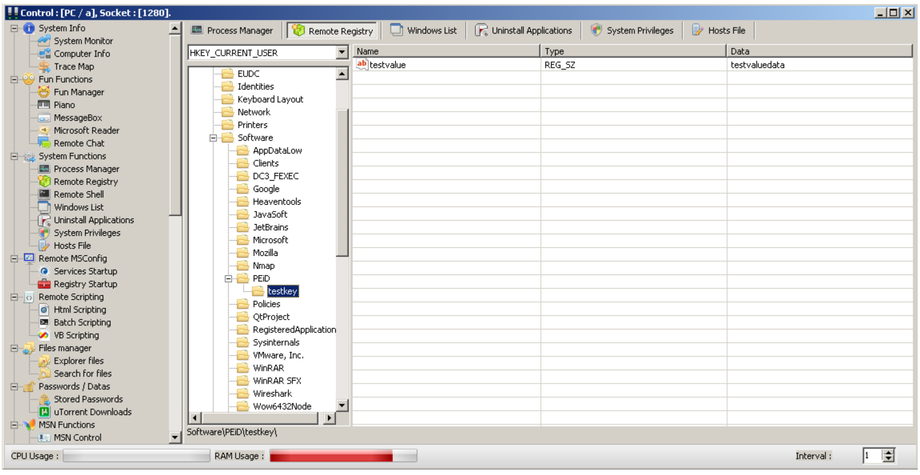

```
...
dwm.exe|ACCESS DENIED (x64)|3|2196|1597440|a\pc|872|Normal|4424
explorer.exe|ACCESS DENIED (x64)|39|4080|35332096|a\pc|3844|Normal|4424
vmtoolsd.exe|ACCESS DENIED (x64)|6|4880|9121792|a\pc|4080|Normal|4424
jusched.exe|C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe|2|3740|2023424|a\pc|4364|Normal|4424
jucheck.exe|C:\Program Files (x86)\Common Files\Java\Java Update\jucheck.exe|9|1056|3973120|a\pc|3740|Normal|4424
chrome.exe|ACCESS DENIED (x64)|33|2704|55390208|a\pc|4080|Normal|4424
chrome.exe|ACCESS DENIED (x64)|7|1300|1515520|a\pc|2704|Normal|4424
chrome.exe|ACCESS DENIED (x64)|2|2956|1654784|a\pc|2704|Normal|4424
...
```

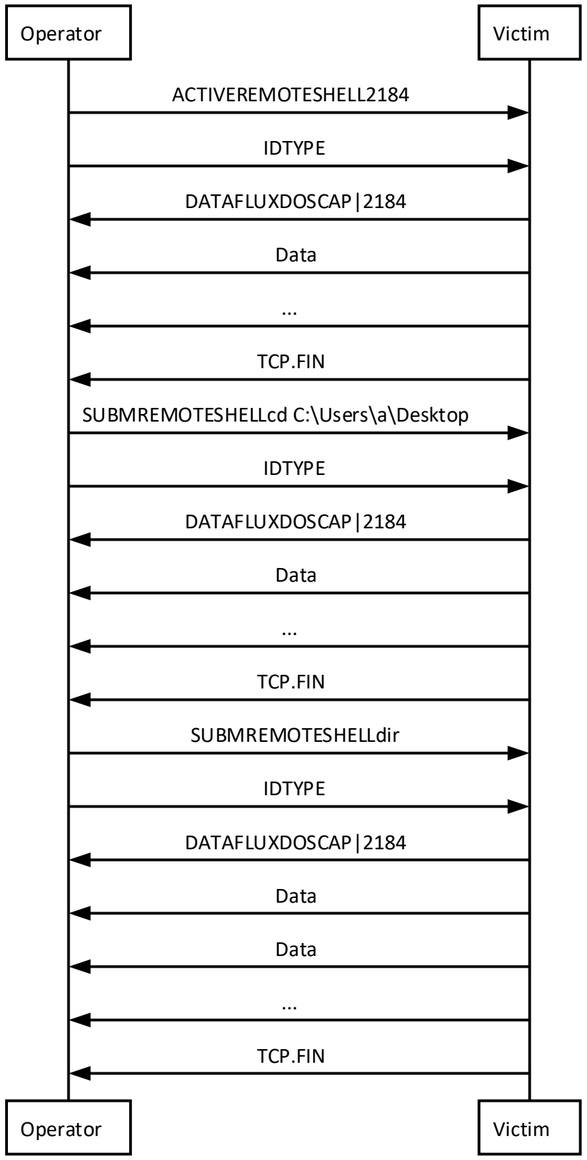
```
...
dwm.exe|ACCESS DENIED (x64)|3|2196|1597440|a\pc|872|Normal|4424
explorer.exe|ACCESS DENIED (x64)|39|4080|35332096|a\pc|3844|Normal|4424
vmtoolsd.exe|ACCESS DENIED (x64)|6|4880|9121792|a\pc|4080|Normal|4424
jusched.exe|C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe|2|3740|2023424|a\pc|4364|Normal|4424
chrome.exe|ACCESS DENIED (x64)|33|2704|55390208|a\pc|4080|Normal|4424
chrome.exe|ACCESS DENIED (x64)|7|1300|1515520|a\pc|2704|Normal|4424
chrome.exe|ACCESS DENIED (x64)|2|2956|1654784|a\pc|2704|Normal|4424
...
```

```
C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe (0x00092000)
C:\Windows\SysWOW64\ntdll.dll (0x00180000)
C:\Windows\syswow64\kernel32.dll (0x00110000)
C:\Windows\syswow64\KERNELBASE.dll (0x00047000)
C:\Windows\syswow64\ole32.dll (0x0015C000)
...
```




Operator
Victim
RgBro1|||REGISTRY|1036
IDTYPE
DATAFLUXREGISTRY|1036
Data
...
TCP.FIN
...
Network
Printers
Software
System
Volatile Environment
New Command Set
RgBro1|Software\||REGISTRY|1036
IDTYPE
DATAFLUXREGISTRY|1036
Data
...
TCP.FIN
...
Mozilla
Nmap
PEiD
Policies
QtProject
...
New Command Set
RgBro1|Software\PEiD\||REGISTRY|1036
IDTYPE
DATAFLUXREGISTRY|1036
Data
...
TCP.FIN
|StayOnTop|REG_DWORD|1
SkipNonPE|REG_DWORD|0
Method|REG_DWORD|0
ShellExtension|REG_DWORD|0
...
New Command Set
CRKey1Software\PEiD\testkey
New Command Set
RgBro1|Software\PEiD\||REGISTRY|1036
IDTYPE
DATAFLUXREGISTRY|1036
Data
...
TCP.FIN
testkey
|StayOnTop|REG_DWORD|1
SkipNonPE|REG_DWORD|0
Method|REG_DWORD|0
...
New Command Set
RgBro1|Software\PEiD\testkey\||REGISTRY|1036
IDTYPE
DATAFLUXREGISTRY|1036
Data
...
TCP.FIN
Nothing (container void)
CRVal1|Software\PEiD\testkey\|testvalue|testvaluedata
New Command Set
RgBro1|Software\PEiD\testkey\||REGISTRY|1036
IDTYPE
DATAFLUXREGISTRY|1036
Data
...
TCP.FIN
|testvalue|REG_SZ|testvaluedata
New Command Set
DRVal1Software\PEiD\testkey*testvalue
New Command Set
DRKey1Software\PEiD\testkey\
New Command Set
RgBro1|Software\PEiD\||REGISTRY|1036
IDTYPE
DATAFLUXREGISTRY|1036
Data
...
TCP.FIN
|StayOnTop|REG_DWORD|1
SkipNonPE|REG_DWORD|0
Method|REG_DWORD|0
ShellExtension|REG_DWORD|0
...
Operator
Victim


Control : [PC / a], Socket : [1280].
System Info
System Monitor
Computer Info
Trace Map
Fun Functions
Fun Manager
Piano
MessageBox
Microsoft Reader
Remote Chat
System Functions
Process Manager
Remote Registry
Remote Shell
Windows List
Uninstall Applications
System Privileges
Hosts File
Remote MSConfig
Services Startup
Registry Startup
Remote Scripting
Html Scripting
Batch Scripting
VB Scripting
Files manager
Explorer files
Search for files
Passwords / Datas
Stored Passwords
uTorrent Downloads
MSN Functions
MSN Control
Process Manager
Remote Registry
Windows List
Uninstall Applications
System Privileges
Hosts File
HKEY_CURRENT_USER
EUDC
Identities
Keyboard Layout
Network
Printers
Software
AppDataLow
Clients
DC3_FEXEC
Google
Heaventools
JavaSoft
JetBrains
Microsoft
Mozilla
Nmap
PEiD
testkey
Policies
QtProject
RegisteredApplication
Sysinternals
VMware, Inc.
WinRAR
WinRAR SFX
Wireshark
Wow6432Node
Name
Type
Data
testvalue
REG_SZ
testvaluedata
Software\PEiD\testkey\
CPU Usage :
RAM Usage :
Interval :
1



Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\a\Desktop\dc\stubs\chrome>

cd C:\Users\a\Desktop

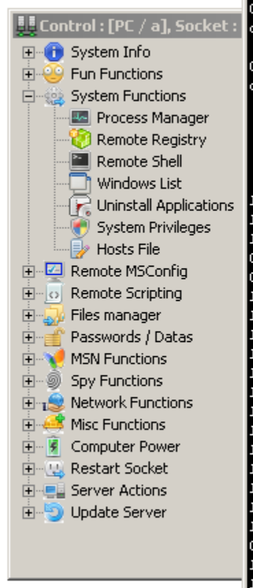
C:\Users\a\Desktop>

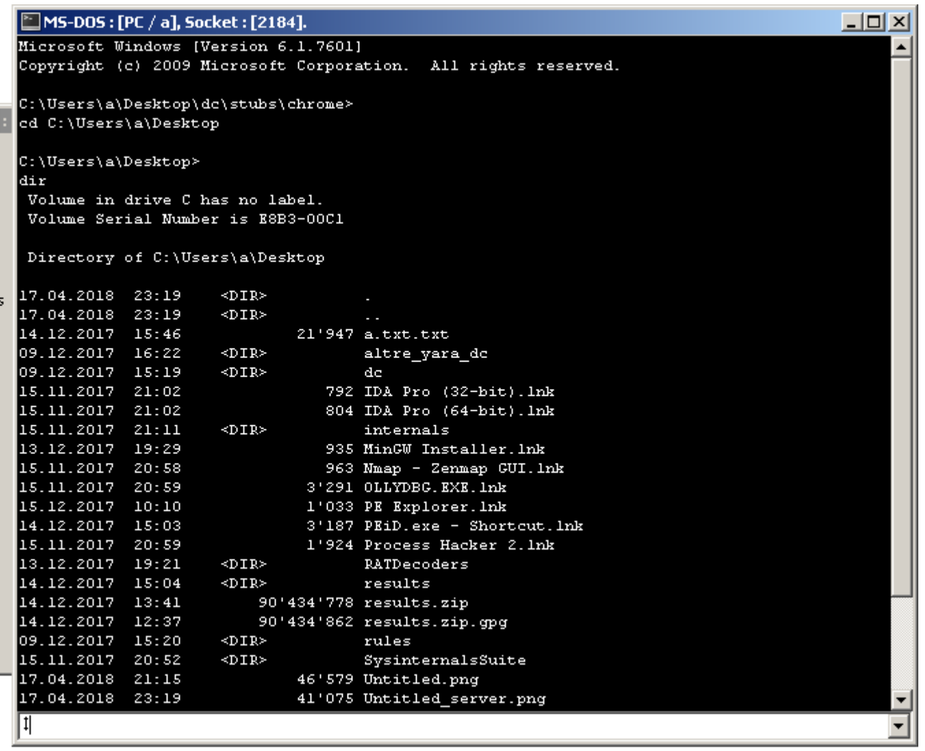
dir
 Volume in drive C has no label.
 Volume Serial Number is E8B3-00C1

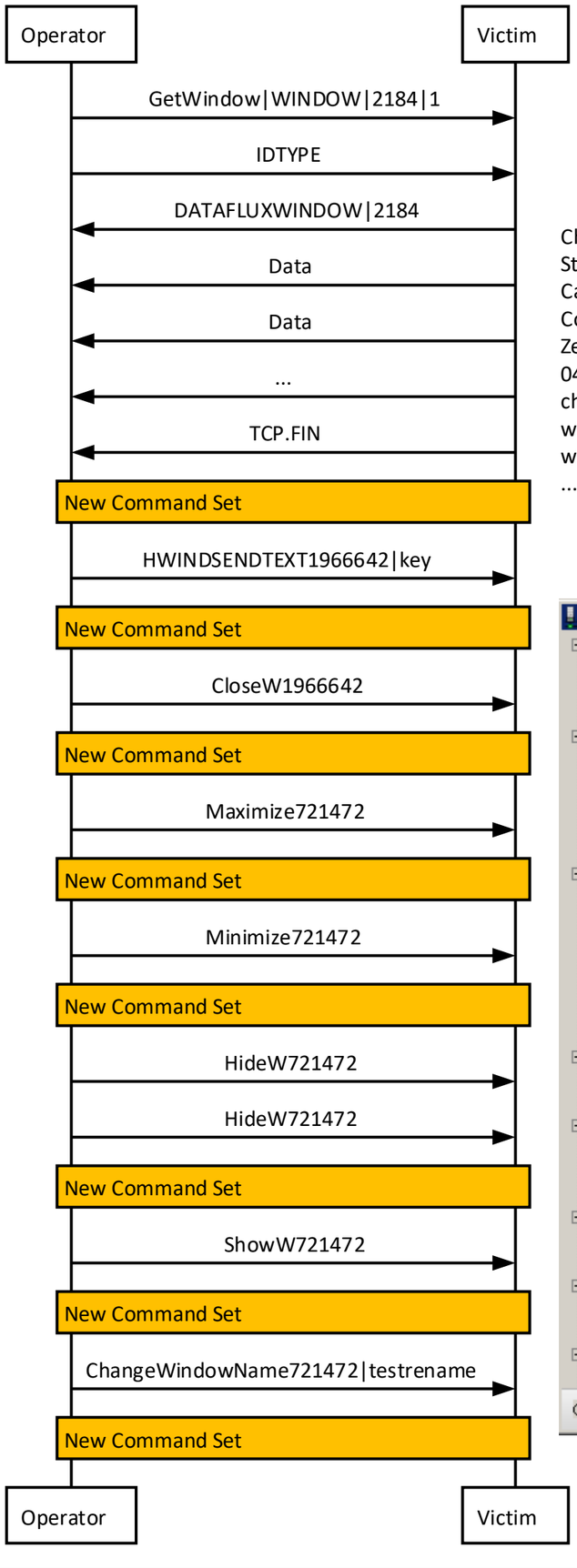
 Directory of C:\Users\a\Desktop

17.04.2018 23:19   <DIR>   .
17.04.2018 23:19   <DIR>   ..
14.12.2017 15:46   21'947 a.txt.txt
09.12.2017 16:22   <DIR>   altre_yara_dc
09.12.2017 15:19   <DIR>   dc
15.11.2017 21:02   792 IDA Pro (32-bit).lnk
15.11.2017 21:02   804 IDA Pro (64-bit).lnk
15.11.2017 21:11   <DIR>   internals
13.12.2017 19:29   935 MinGW Installer.lnk
15.11.2017 20:58   963 Nmap - Zenmap GUI.lnk
15.11.2017 20:59   3'291 OLLYDBG.EXE.lnk
15.12.2017 10:10   1'033 PE Explorer.lnk
14.12.2017 15:03   3'187 PEiD.exe - Shortcut.lnk
15.11.2017 20:59   1'924 Process Hacker 2.lnk
13.12.2017 19:21   <DIR>   RATDecoders
14.12.2017 15:04   <DIR>   results
14.12.2017 13:41   90'434'778 results.zip
14.12.2017 12:37   90'434'862 results.zip.gpg
09.12.2017 15:20   <DIR>   rules
15.11.2017 20:52   <DIR>   SysinternalsSuite
17.04.2018 21:15   46'579 Untitled.png
17.04.2018 23:19   41'075 Untitled_server.png
13.12.2017 18:39   <DIR>   yara-python
              13 File(s)   180'992'170 bytes
              10 Dir(s) 36'032'405'504 bytes free

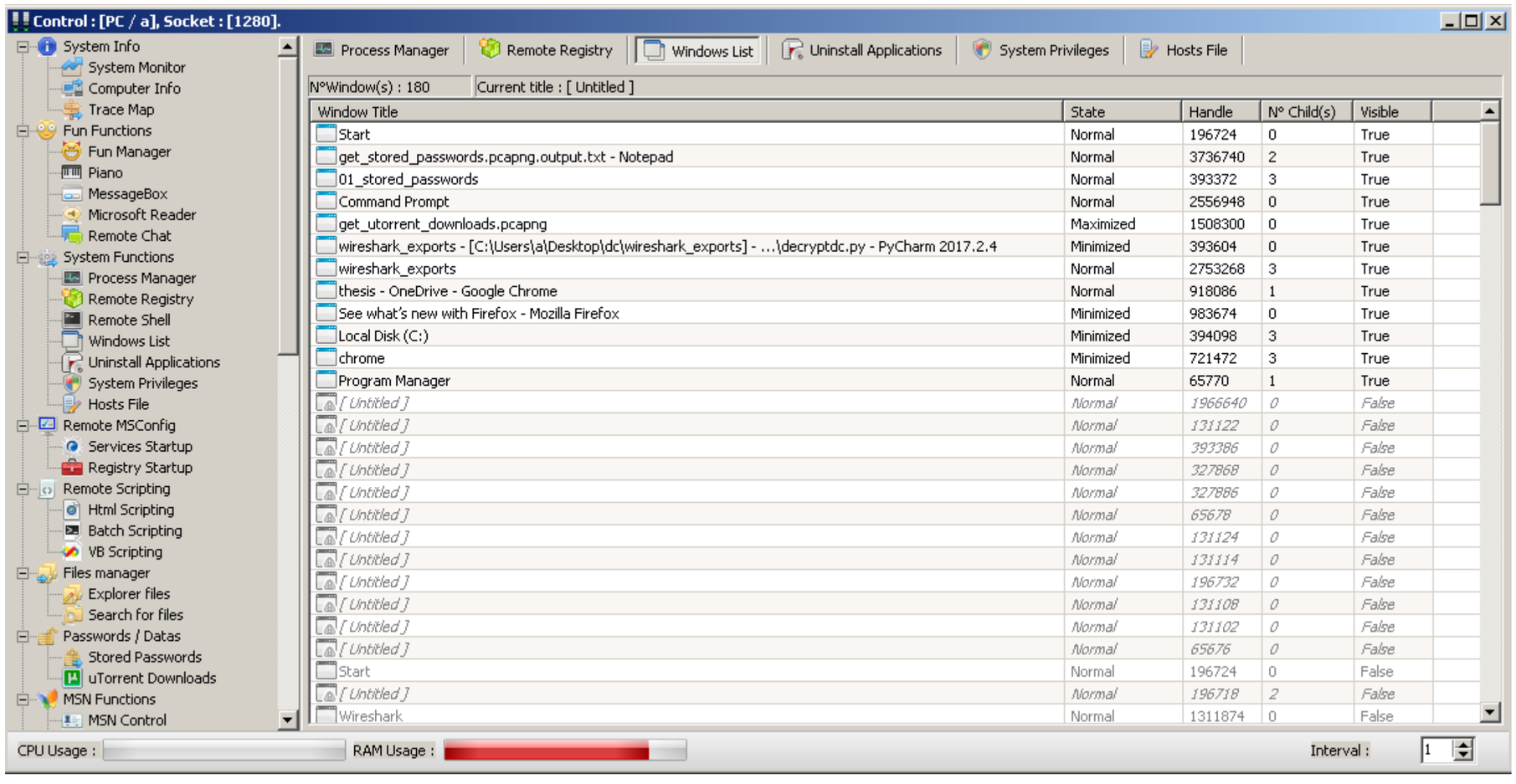
C:\Users\a\Desktop>



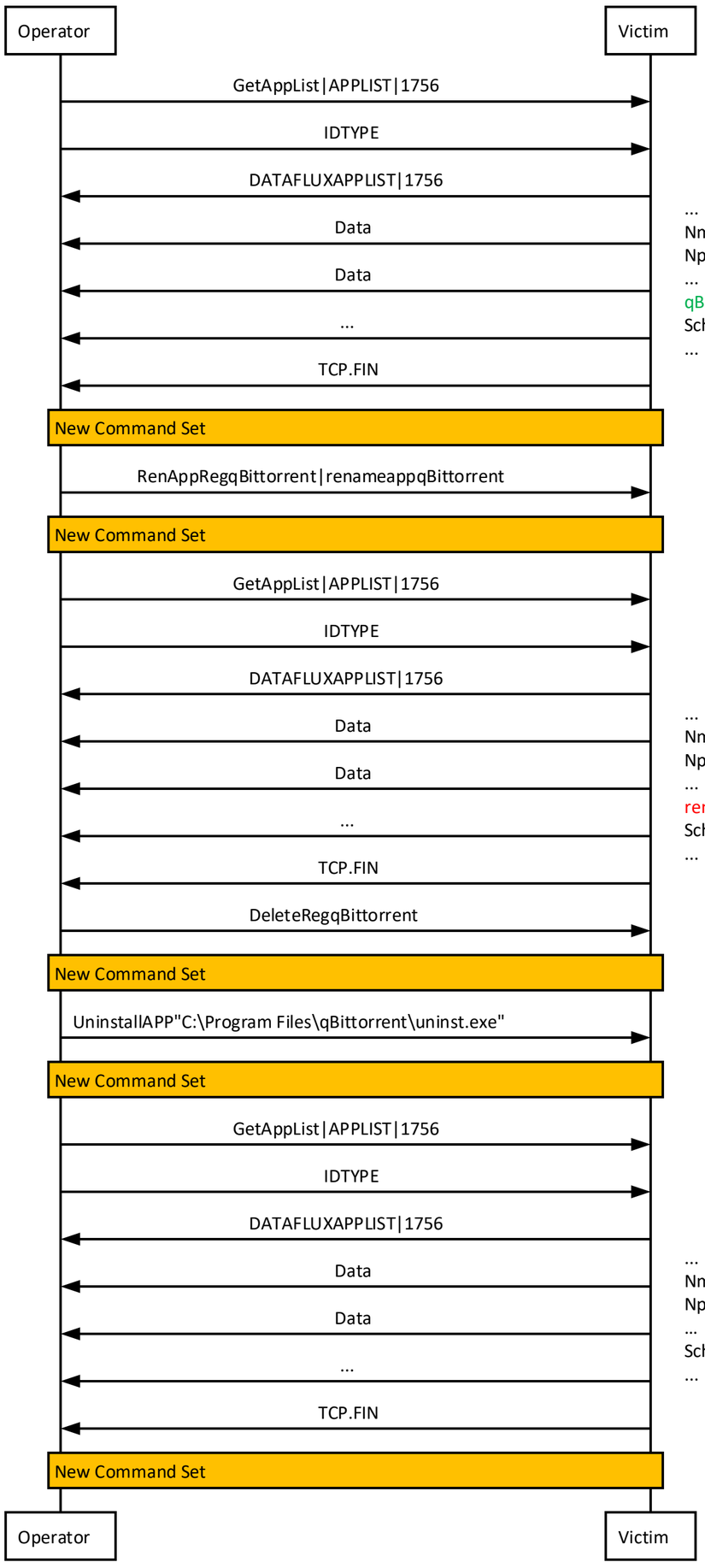




Chat|Normal|394026|2|True
Start|Normal|196724|0|True
Cattura da Local Area Connection|Maximized|1508300|0|True
Command Prompt|Normal|2556948|0|True
Zenmap|Normal|1966642|0|True
04_windows_list|Normal|393372|3|True
chrome|Minimized|721472|3|True
wireshark_exports - [C:\Users\a\Desktop\dc\wireshark_exports] - ...\decryptdc.py - PyCharm 2017.2.4|Minimized|393604|0|True
wireshark_exports|Normal|2753268|3|True
...



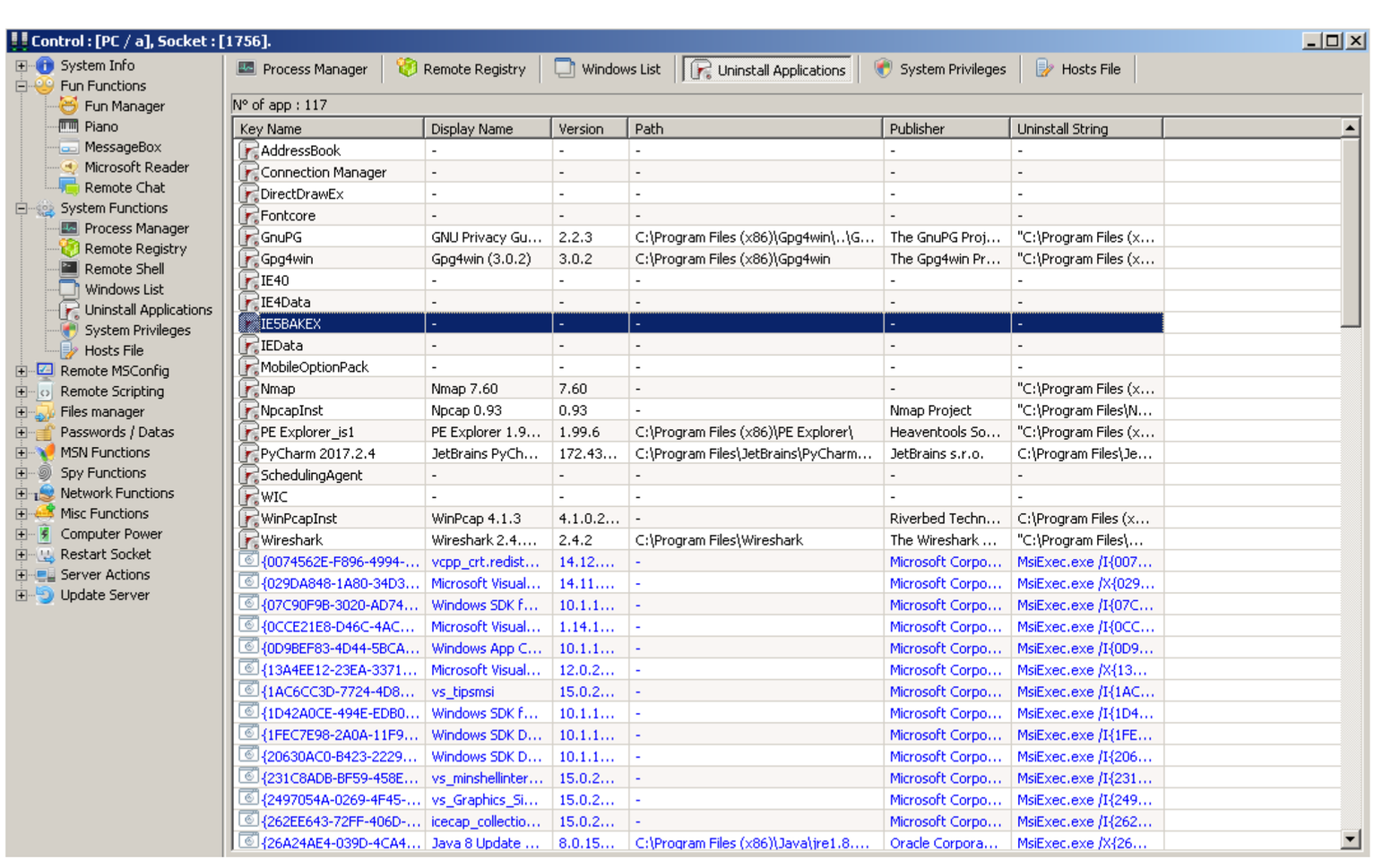
System Functions -> Uninstall Applications



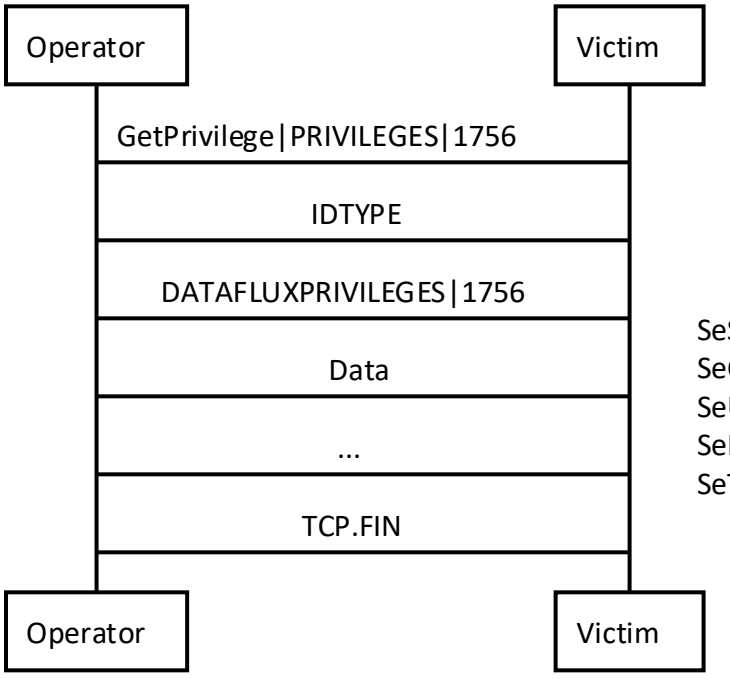
...
Nmap|Nmap 7.60|7.60|||"C:\Program Files (x86)\Nmap\uninstall.exe"
NpcapInst|Npcap 0.93|0.93||Nmap Project|"C:\Program Files\Npcap\uninstall.exe"
...
qBittorrent|qBittorrent 4.0.2|4.0.2||The qBittorrent project|"C:\Program Files\qBittorrent\uninst.exe"
SchedulingAgent|||||
...

...
Nmap|Nmap 7.60|7.60|||"C:\Program Files (x86)\Nmap\uninstall.exe"
NpcapInst|Npcap 0.93|0.93||Nmap Project|"C:\Program Files\Npcap\uninstall.exe"
...
renameappqBittorrent|qBittorrent 4.0.2|4.0.2||The qBittorrent project|"C:\Program Files\qBittorrent\uninst.exe"
SchedulingAgent|||||
...

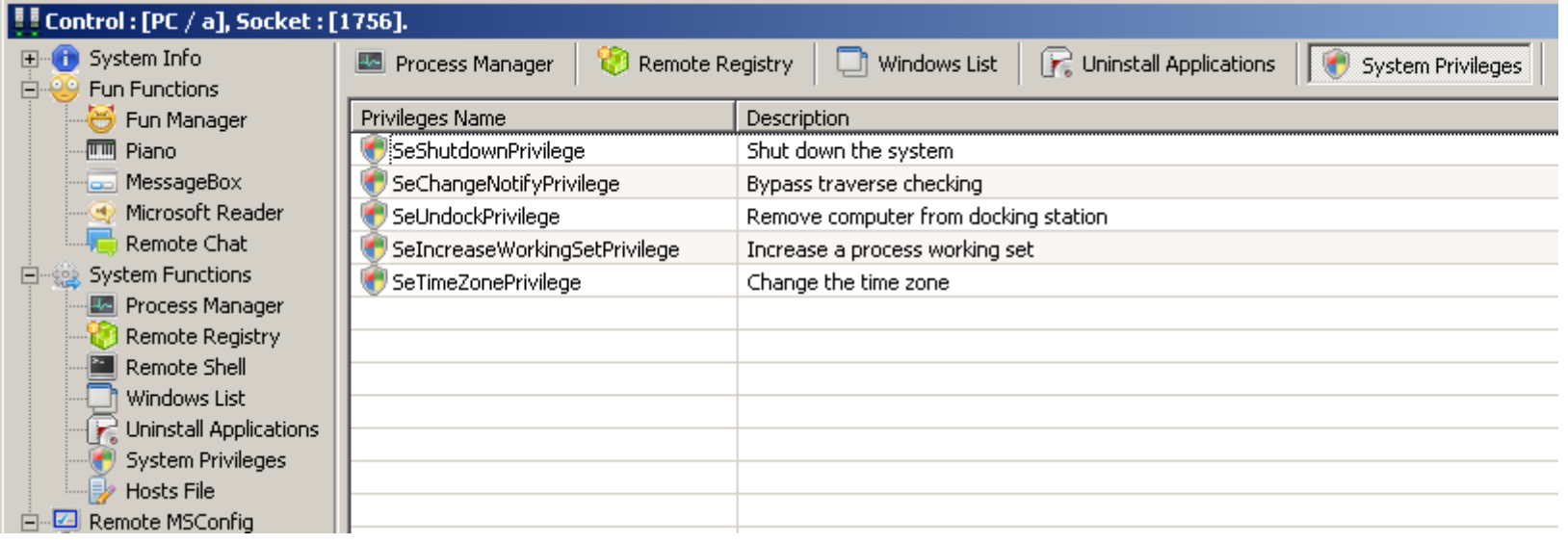
...
Nmap|Nmap 7.60|7.60|||"C:\Program Files (x86)\Nmap\uninstall.exe"
NpcapInst|Npcap 0.93|0.93||Nmap Project|"C:\Program Files\Npcap\uninstall.exe"
...
SchedulingAgent|||||
...



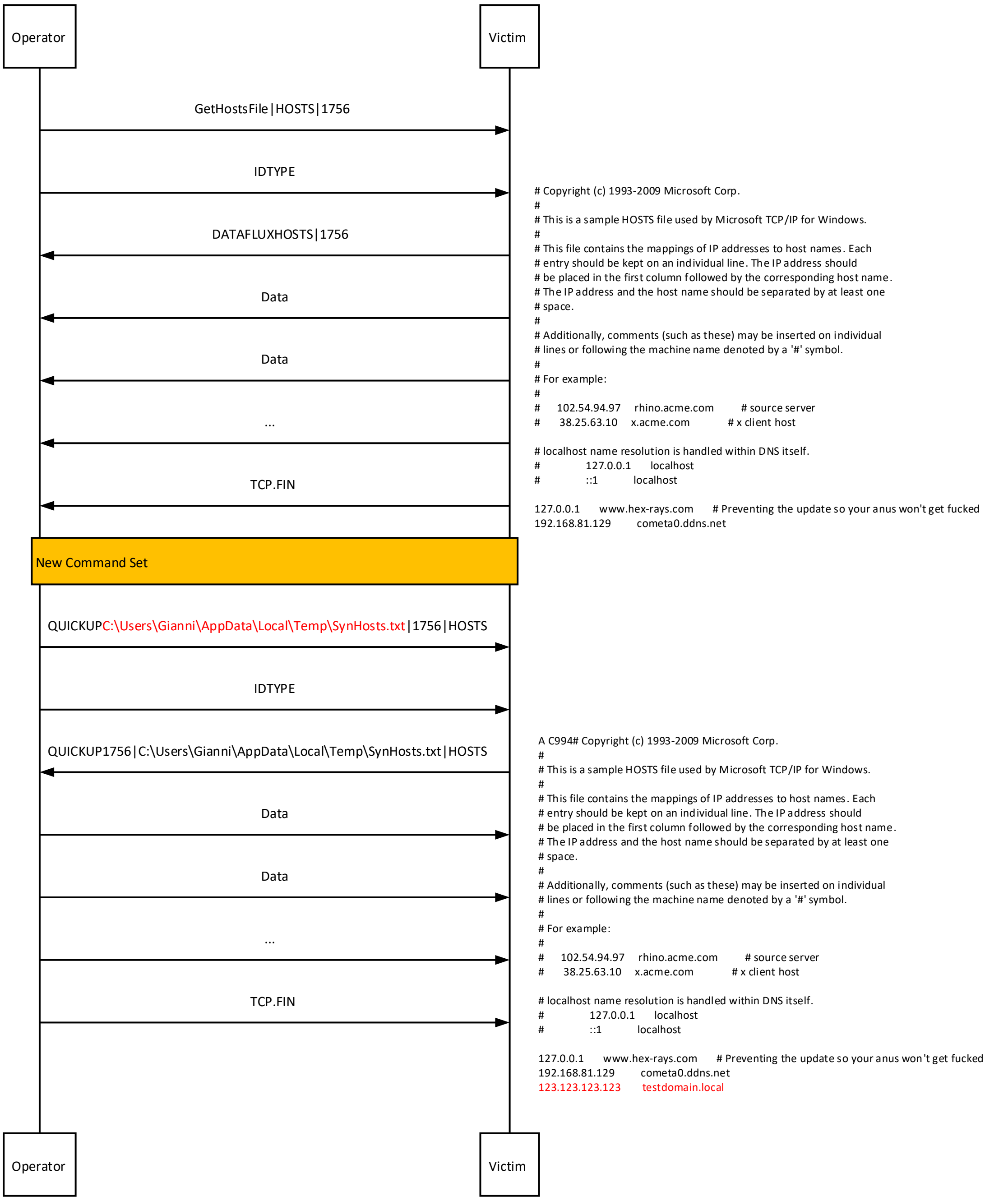
System Functions -> System Privileges



SeShutdownPrivilege|Shut down the system
SeChangeNotifyPrivilege|Bypass traverse checking
SeUndockPrivilege|Remove computer from docking station
SeIncreaseWorkingSetPrivilege|Increase a process working set
SeTimeZonePrivilege|Change the time zone

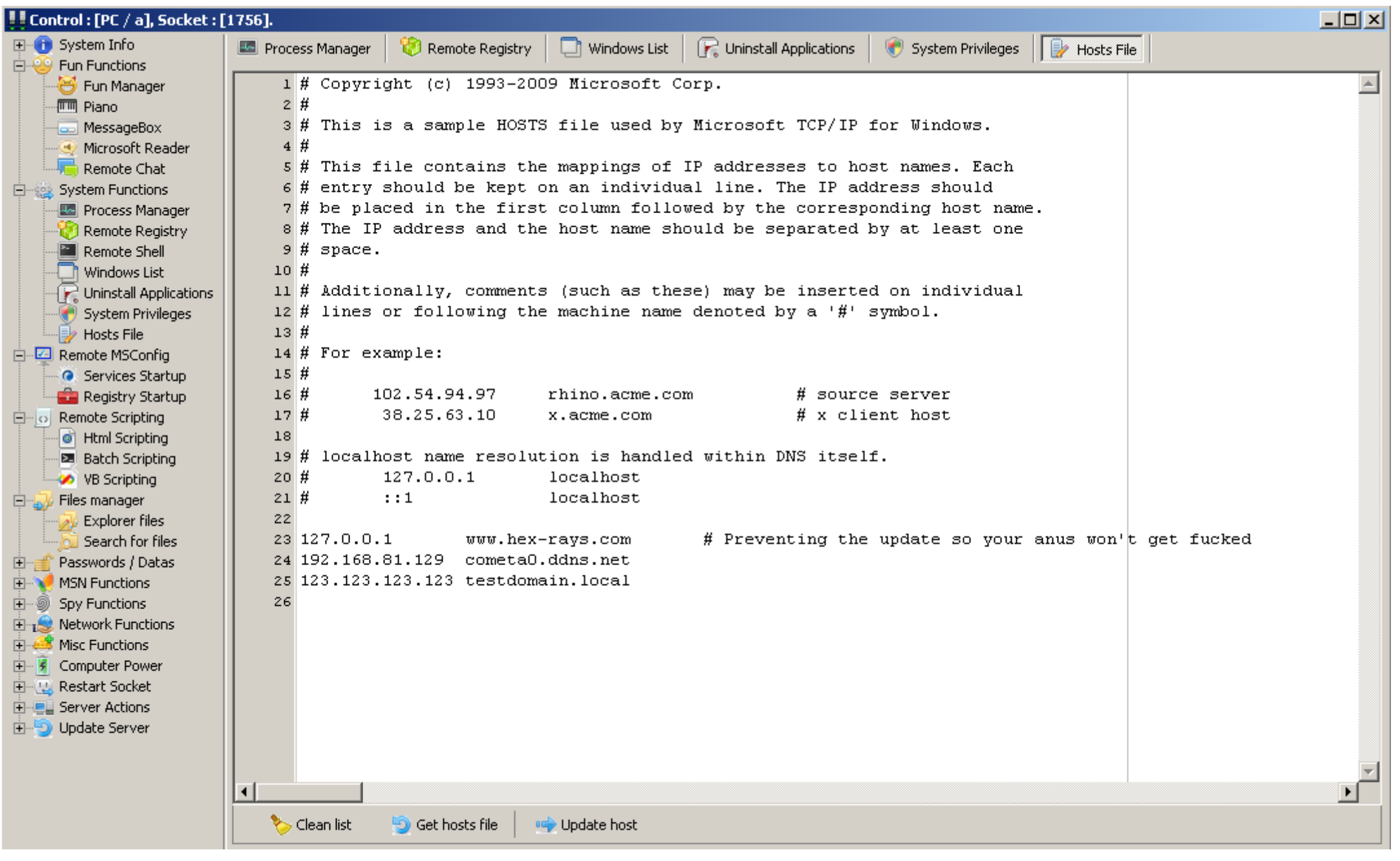


System Functions -> Hosts

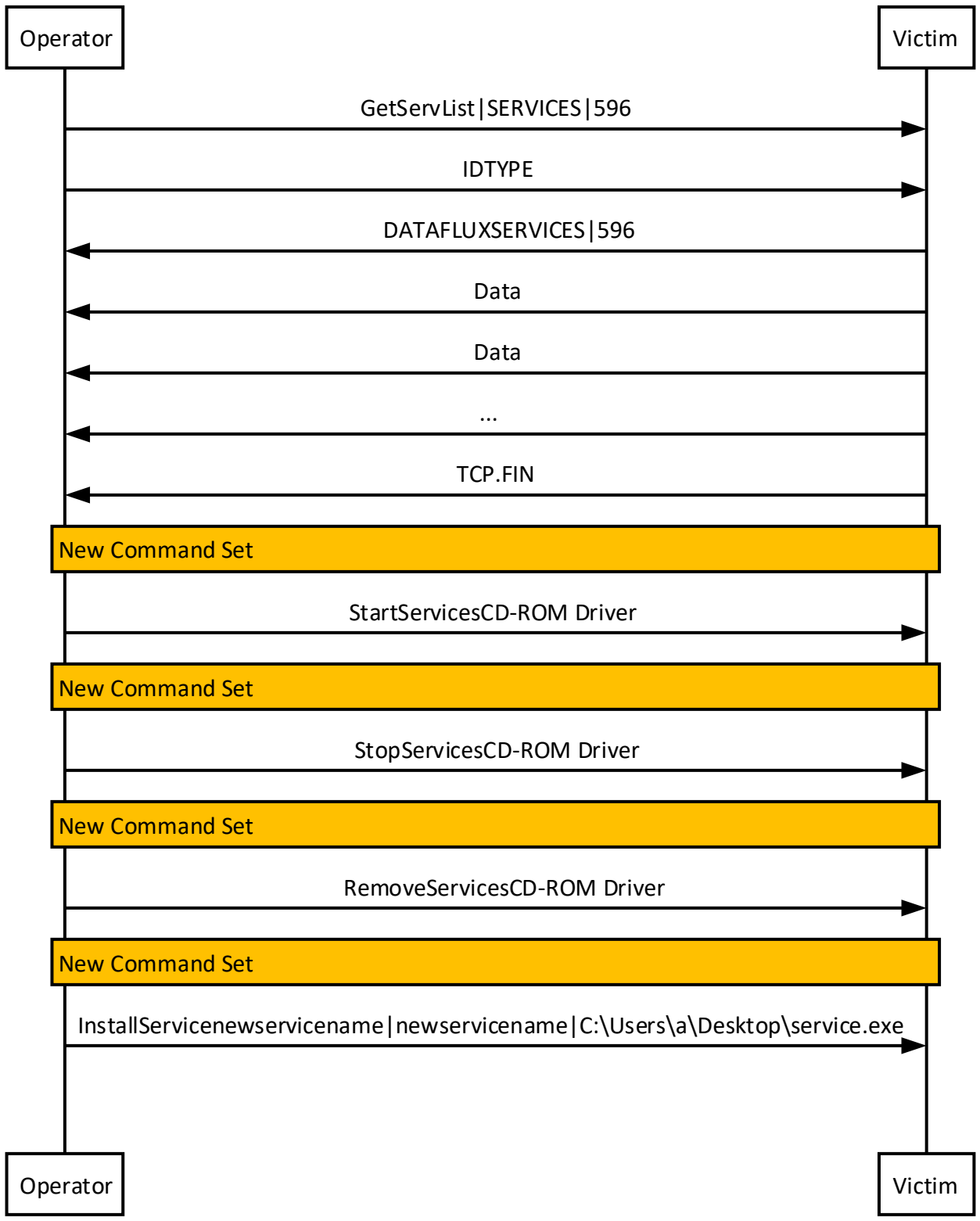



```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the 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

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost

127.0.0.1       www.hex-rays.com       # Preventing the update so your anus won't get fucked
192.168.81.129  cometa0.ddns.net
```

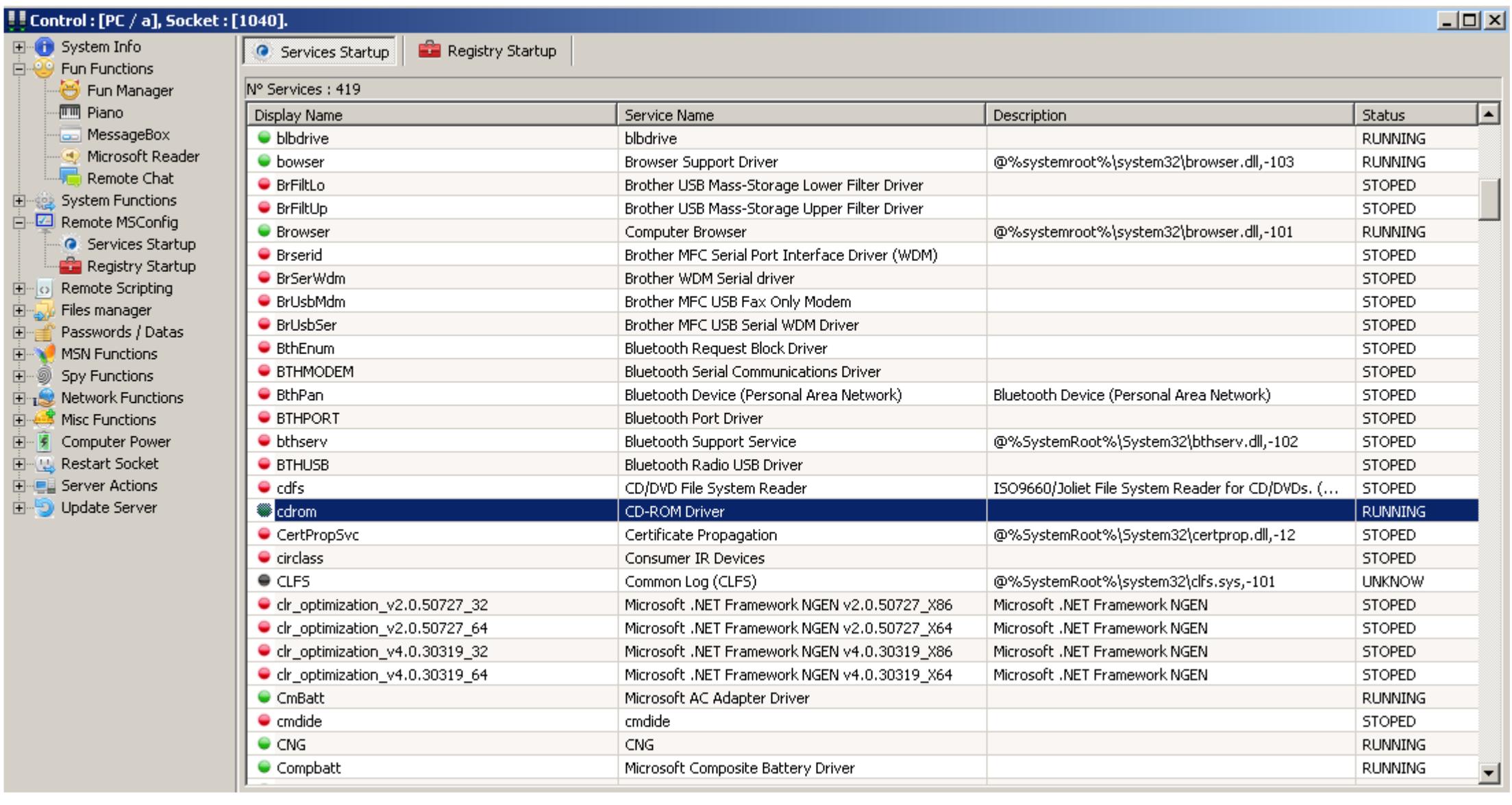
```
A C994# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed 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

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost

127.0.0.1       www.hex-rays.com       # Preventing the update so your anus won't get fucked
192.168.81.129  cometa0.ddns.net
123.123.123.123 testdomain.local
```



Remote MSConfig -> Services Startup

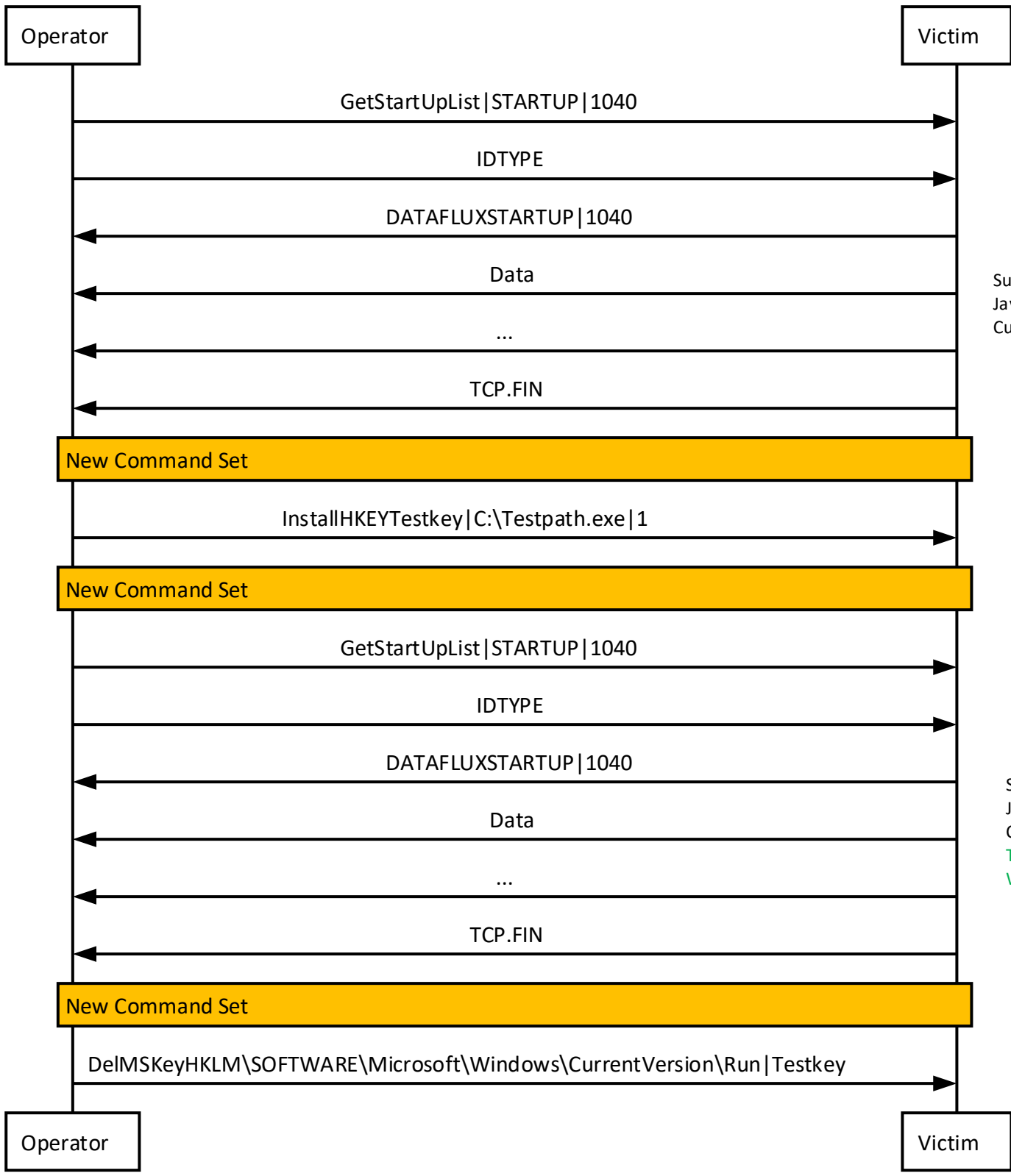


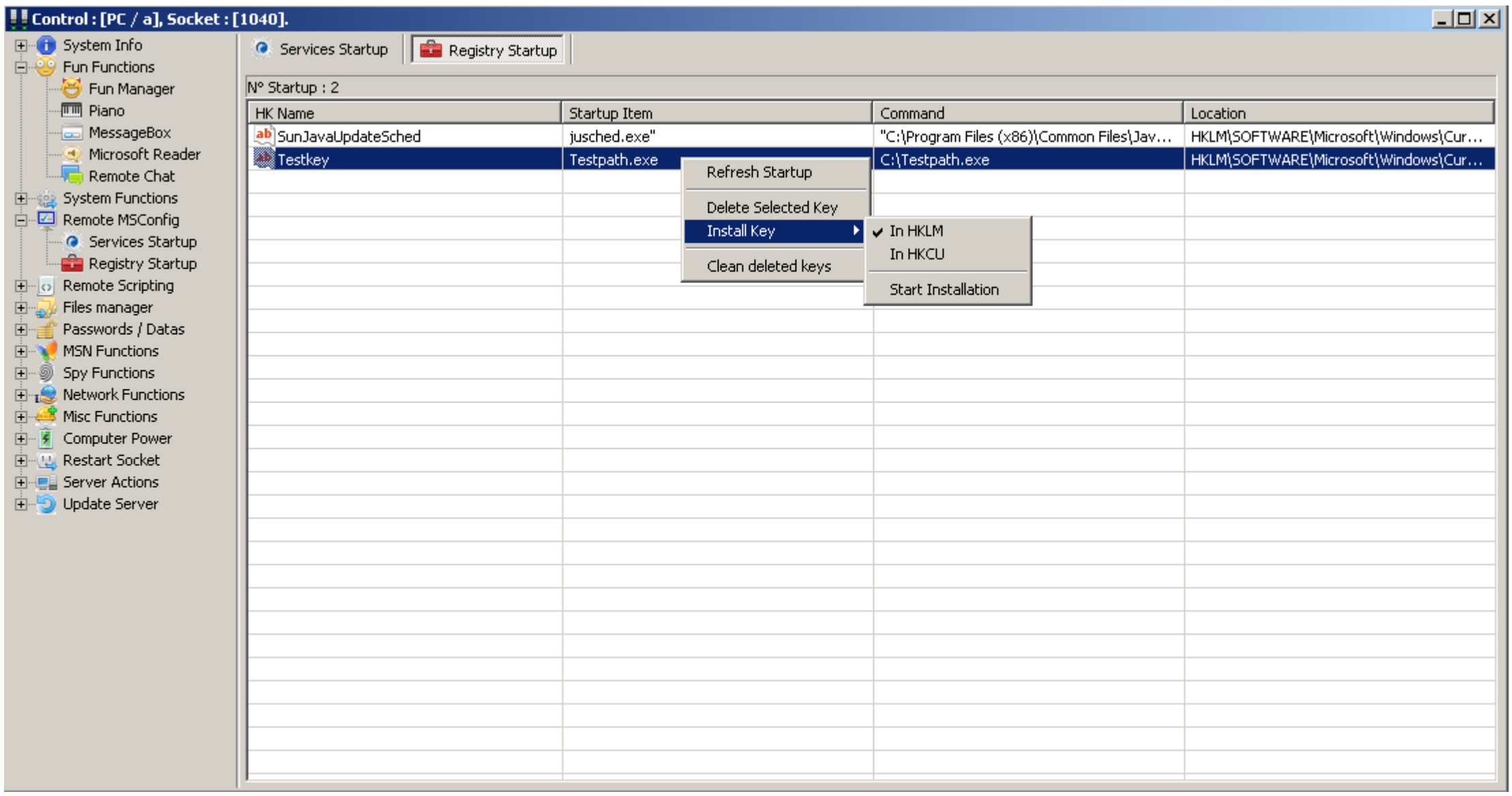
...
cdfs|CD/DVD File System Reader||UNKNOW
cdrom|CD-ROM Driver||UNKNOW
CertPropSvc|Certificate Propagation||UNKNOW
circlass|Consumer IR Devices||UNKNOW
...



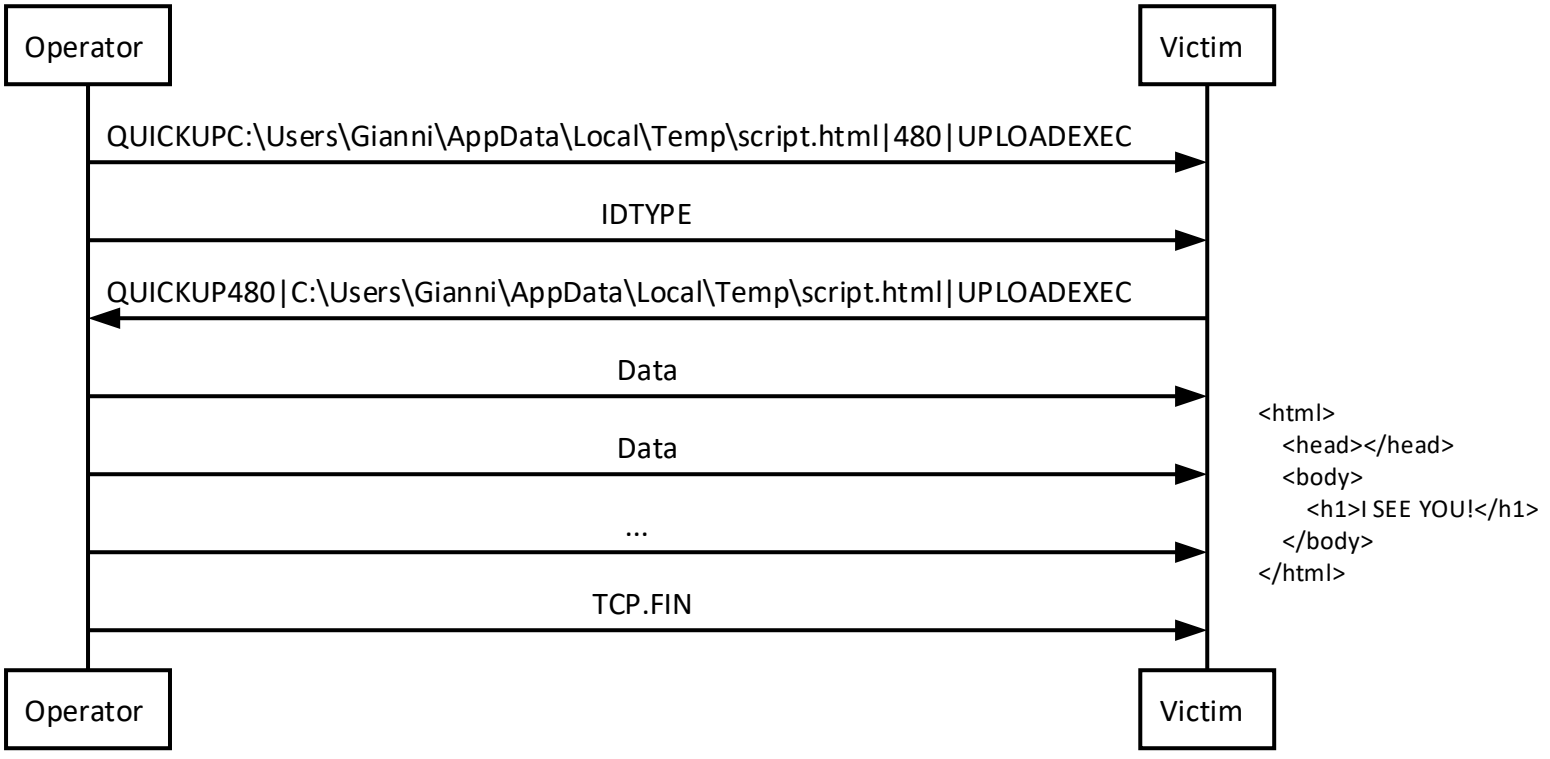
Display Name	Service Name	Description	Status
blbdrive	blbdrive		RUNNING
bowser	Browser Support Driver	@%systemroot%\system32\browser.dll,-103	RUNNING
BrFiltLo	Brother USB Mass-Storage Lower Filter Driver		STOPED
BrFiltUp	Brother USB Mass-Storage Upper Filter Driver		STOPED
Browser	Computer Browser	@%systemroot%\system32\browser.dll,-101	RUNNING
Brserid	Brother MFC Serial Port Interface Driver (WDM)		STOPED
BrSerWdm	Brother WDM Serial driver		STOPED
BrUsbMdm	Brother MFC USB Fax Only Modem		STOPED
BrUsbSer	Brother MFC USB Serial WDM Driver		STOPED
BthEnum	Bluetooth Request Block Driver		STOPED
BTHMODEM	Bluetooth Serial Communications Driver		STOPED
BthPan	Bluetooth Device (Personal Area Network)	Bluetooth Device (Personal Area Network)	STOPED
BTHPORT	Bluetooth Port Driver		STOPED
bthserv	Bluetooth Support Service	@%SystemRoot%\System32\bthserv.dll,-102	STOPED
BTHUSB	Bluetooth Radio USB Driver		STOPED
cdfs	CD/DVD File System Reader	ISO9660/Joliet File System Reader for CD/DVDs. (...	STOPED
cdrom	CD-ROM Driver		RUNNING
CertPropSvc	Certificate Propagation	@%SystemRoot%\System32\certprop.dll,-12	STOPED
circlass	Consumer IR Devices		STOPED
CLFS	Common Log (CLFS)	@%SystemRoot%\system32\clfs.sys,-101	UNKNOW
clr_optimization_v2.0.50727_32	Microsoft .NET Framework NGEN v2.0.50727_X86	Microsoft .NET Framework NGEN	STOPED
clr_optimization_v2.0.50727_64	Microsoft .NET Framework NGEN v2.0.50727_X64	Microsoft .NET Framework NGEN	STOPED
clr_optimization_v4.0.30319_32	Microsoft .NET Framework NGEN v4.0.30319_X86	Microsoft .NET Framework NGEN	STOPED
clr_optimization_v4.0.30319_64	Microsoft .NET Framework NGEN v4.0.30319_X64	Microsoft .NET Framework NGEN	STOPED
CmBatt	Microsoft AC Adapter Driver		RUNNING
cmdide	cmdide		STOPED
CNG	CNG		RUNNING
Compbatt	Microsoft Composite Battery Driver		RUNNING

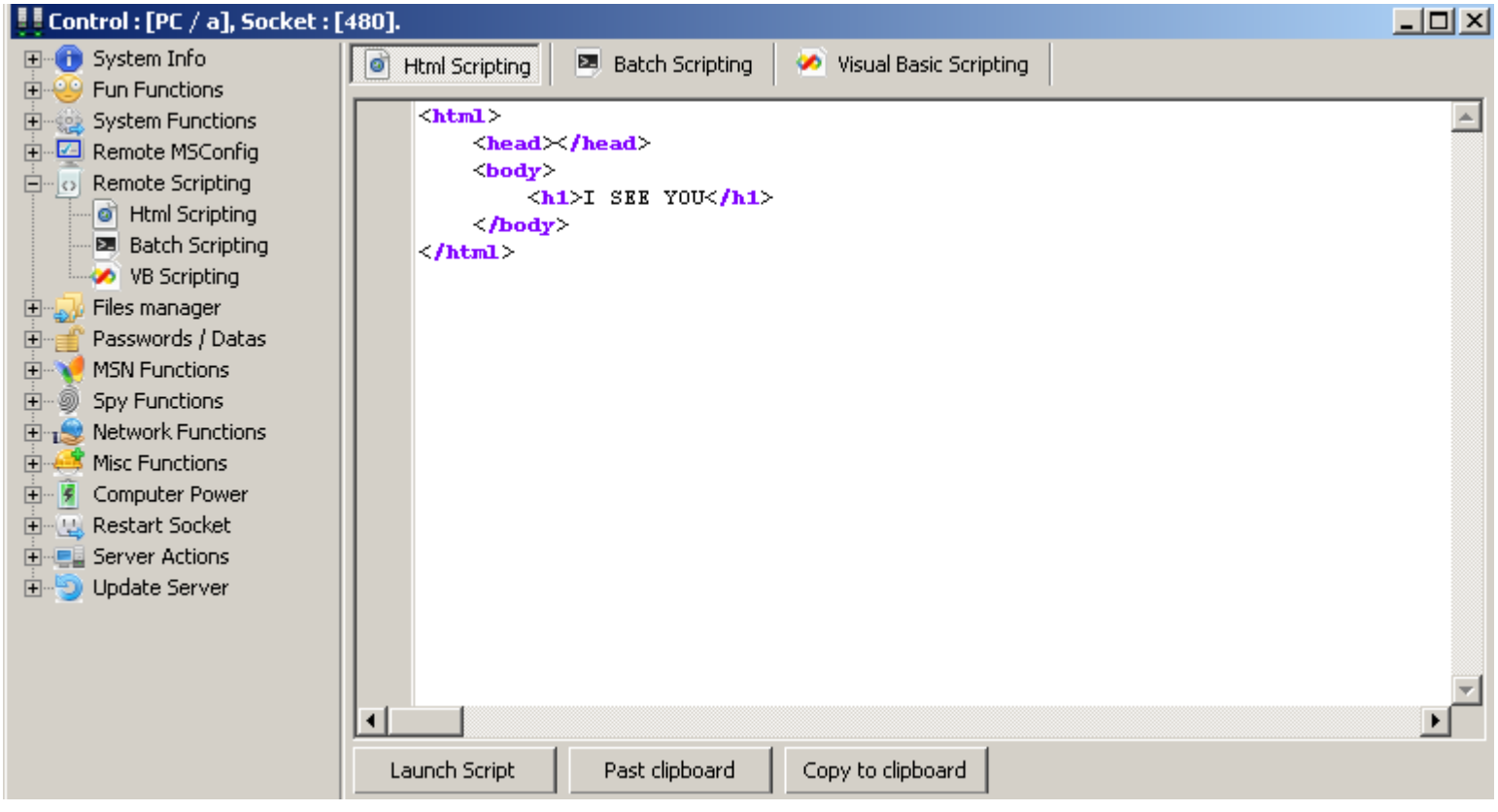
Remote MSConfig -> Registry Startup



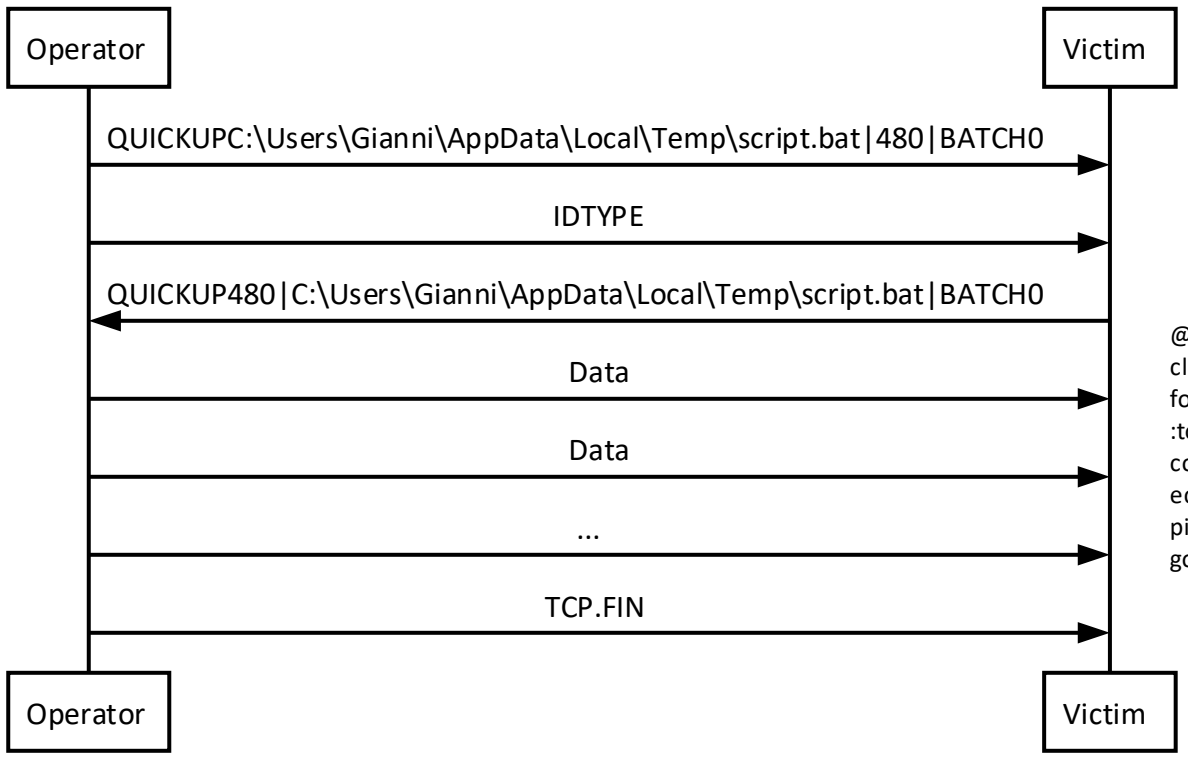


Remote Scripting -> Html Scripting

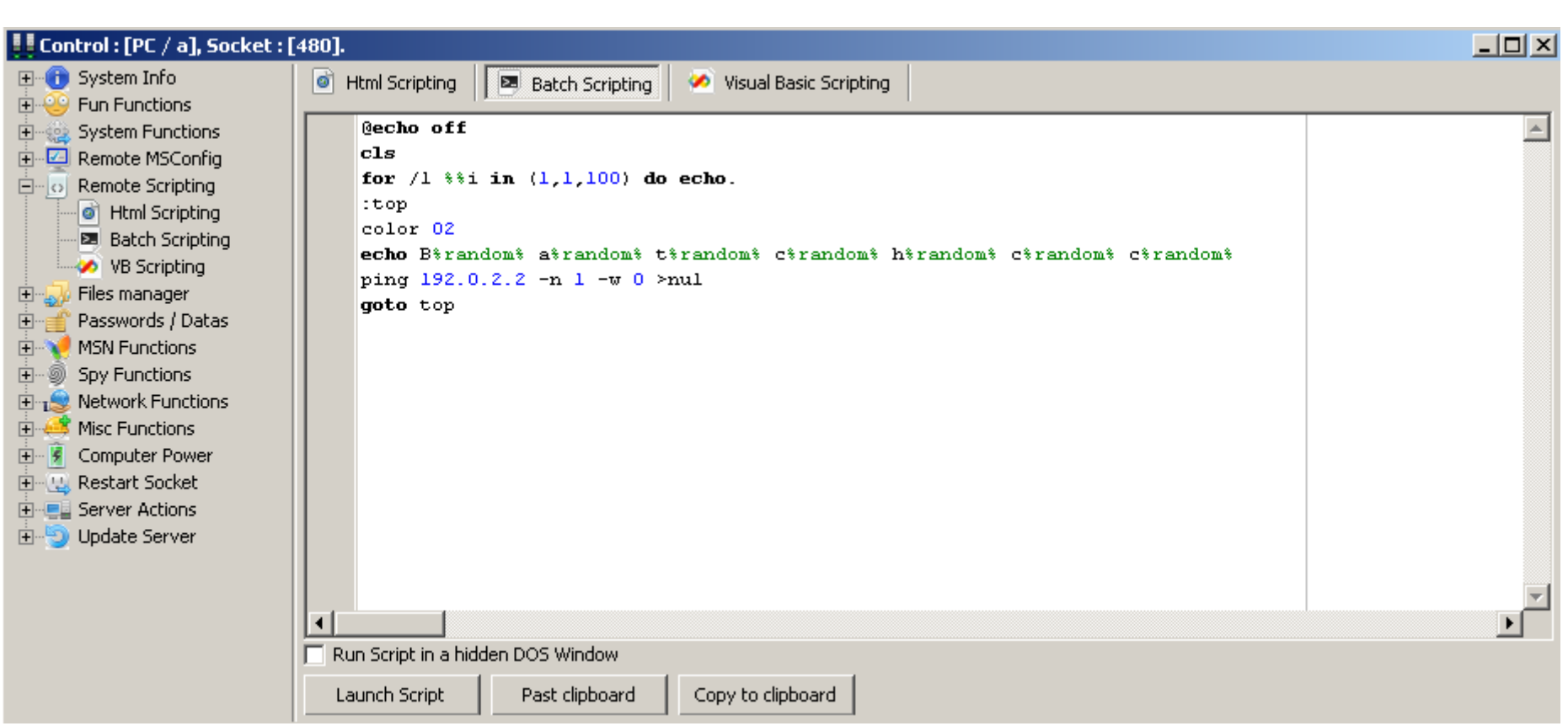




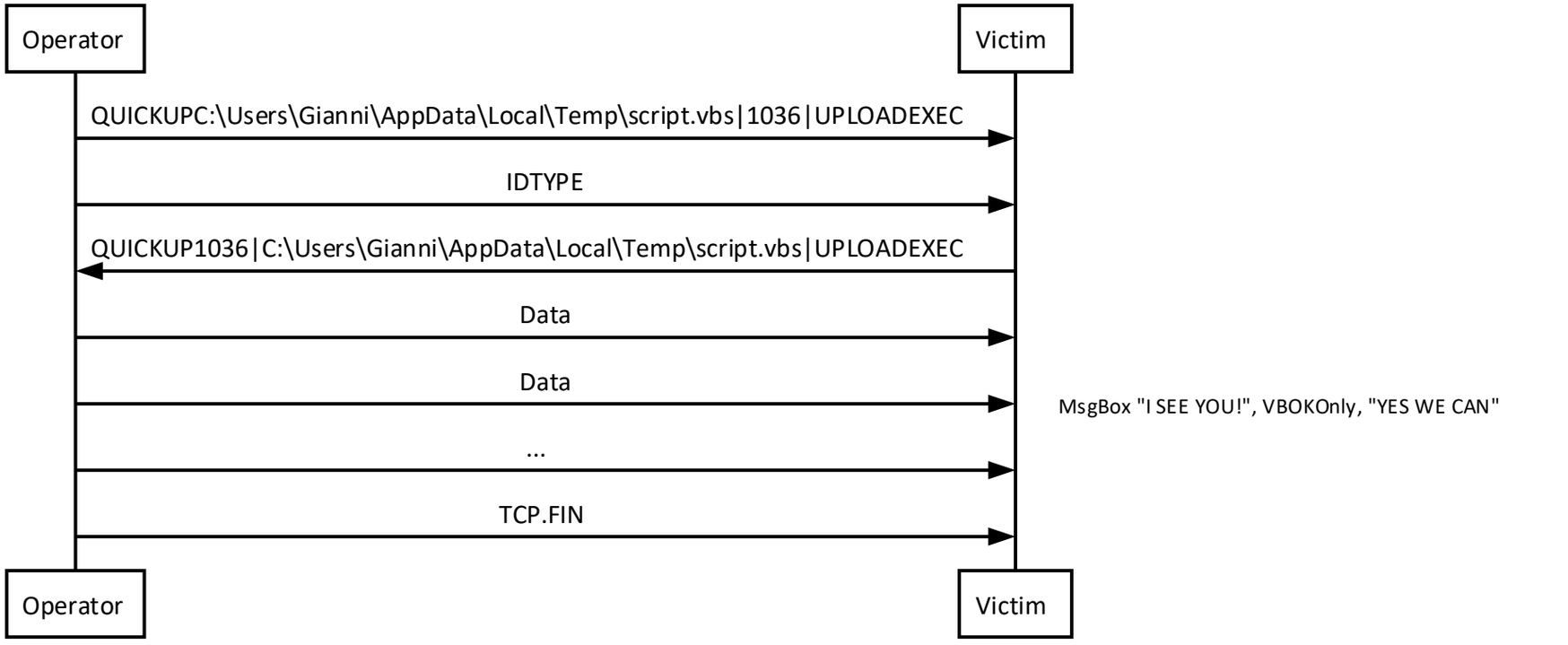
Remote Scripting -> Batch Scripting

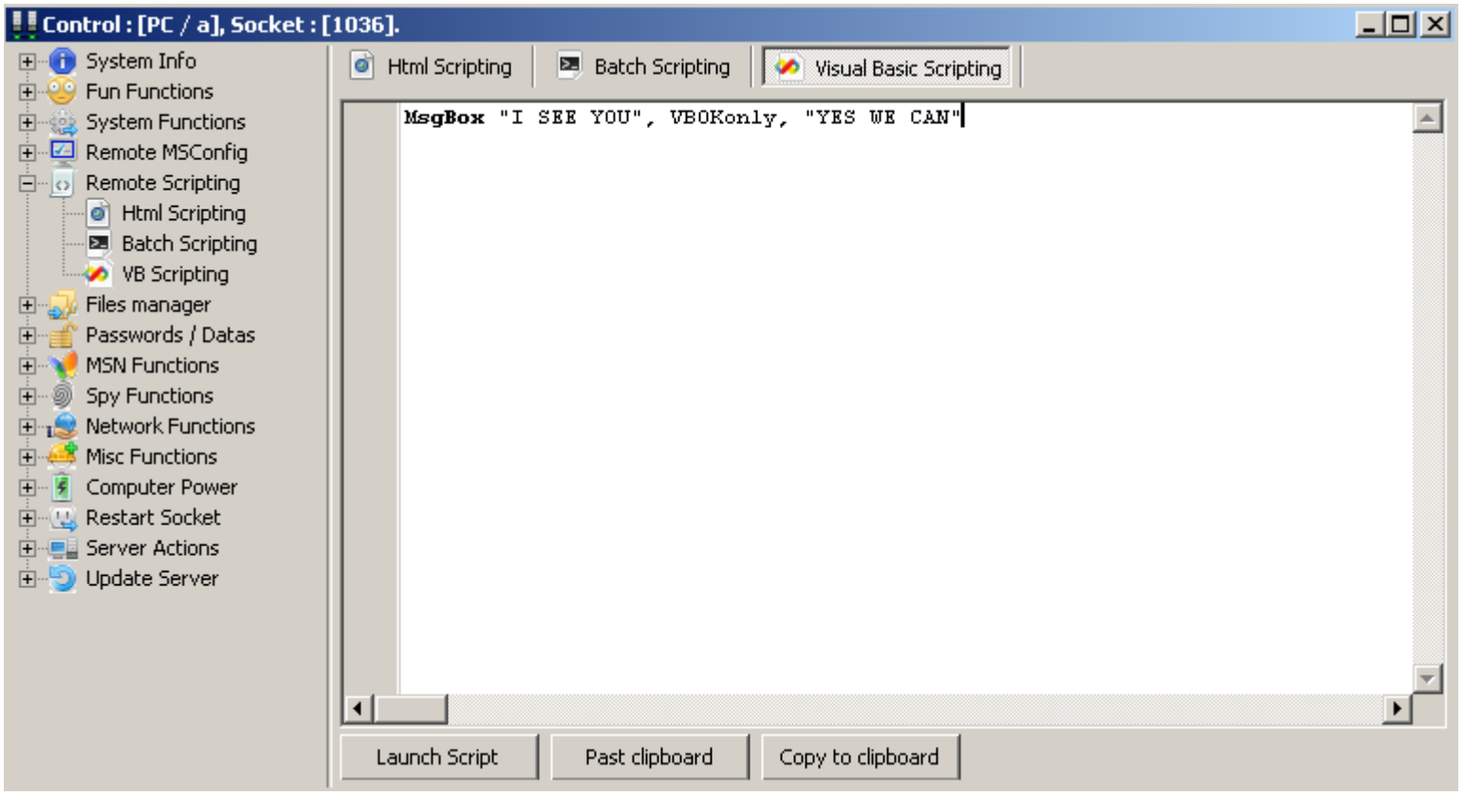



```
@echo off
cls
for /l %%i in (1,1,100) do echo.
:top
color 02
echo B%random% a%random% t%random% c%random% h%random% c%random% c%random%
ping 192.0.2.2 -n 1 -w 0 >nul
goto top
```

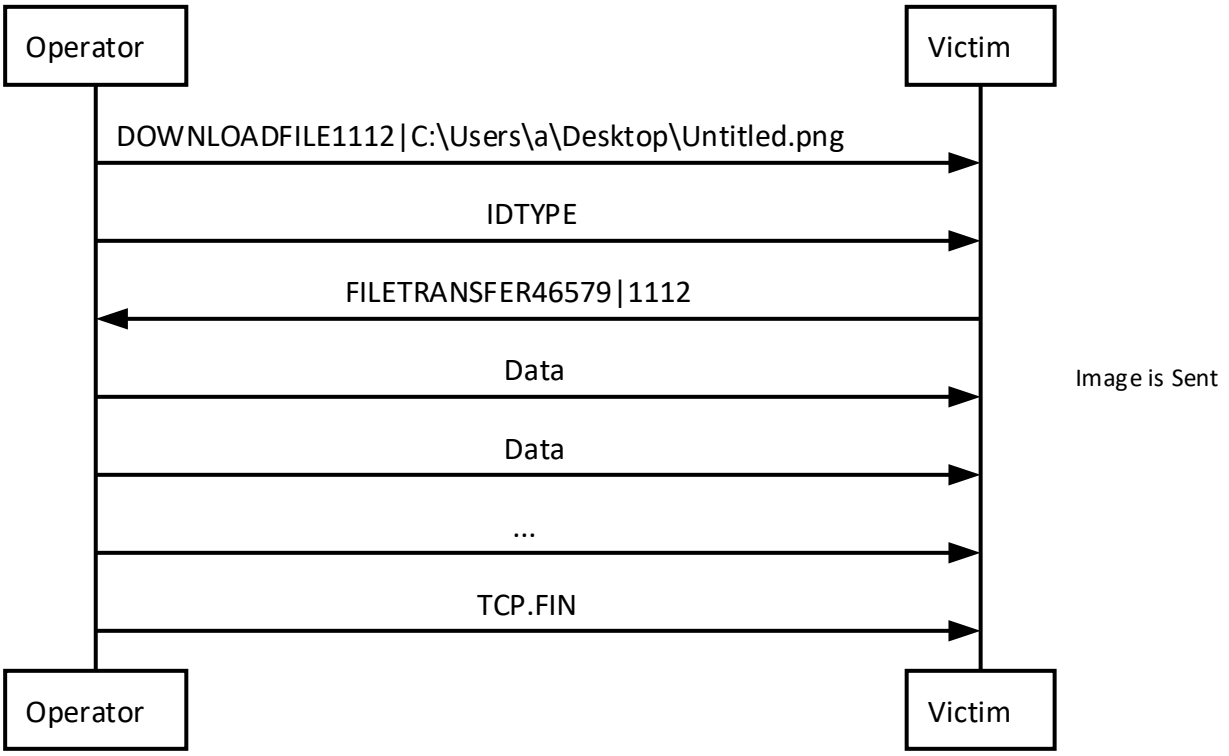


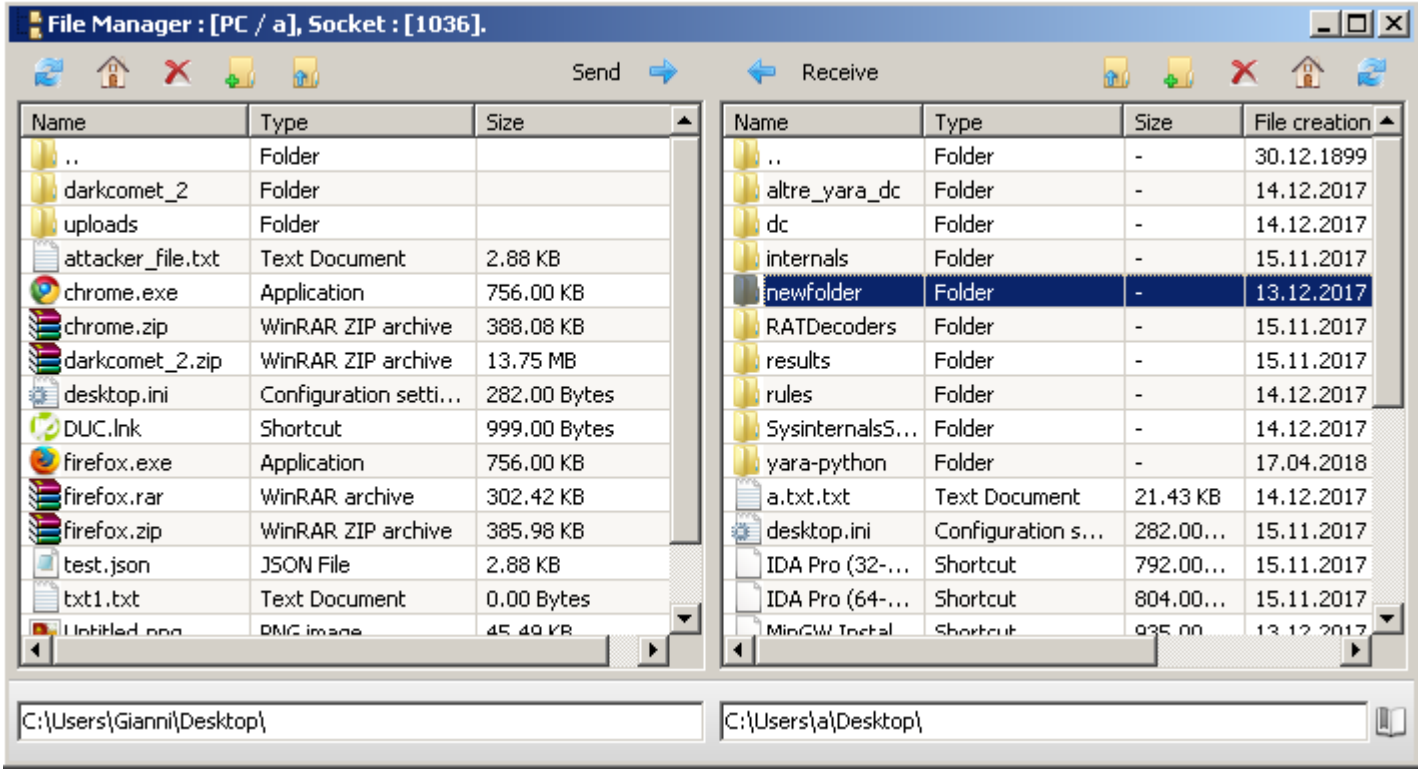
Remote Scripting -> Visual Basic Scripting



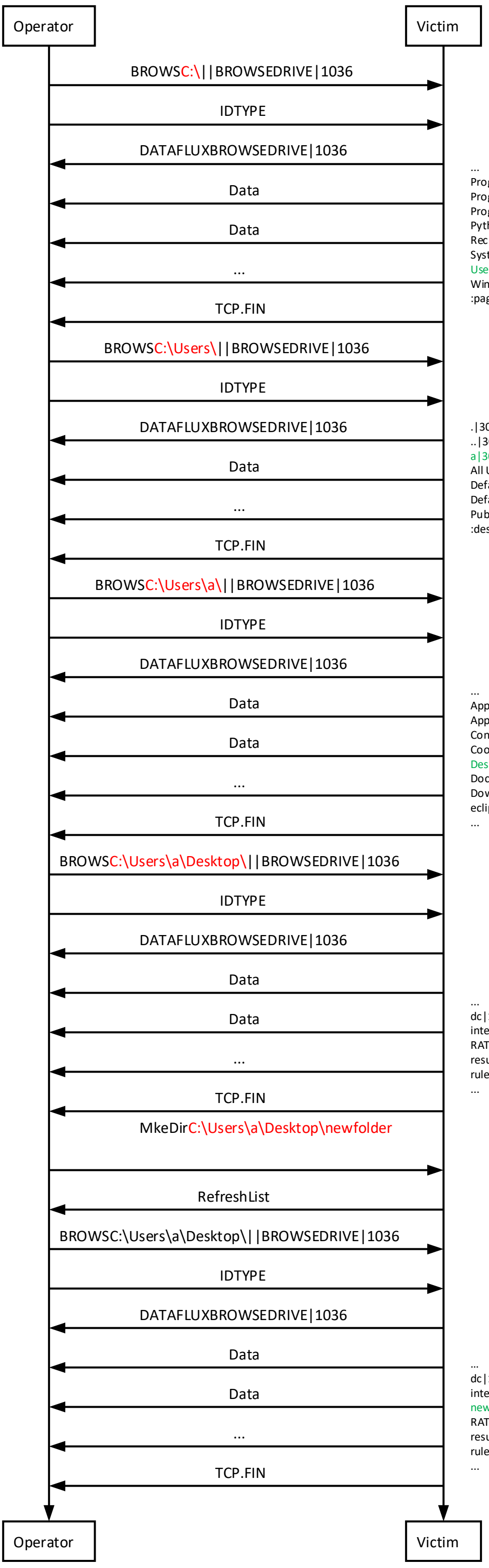


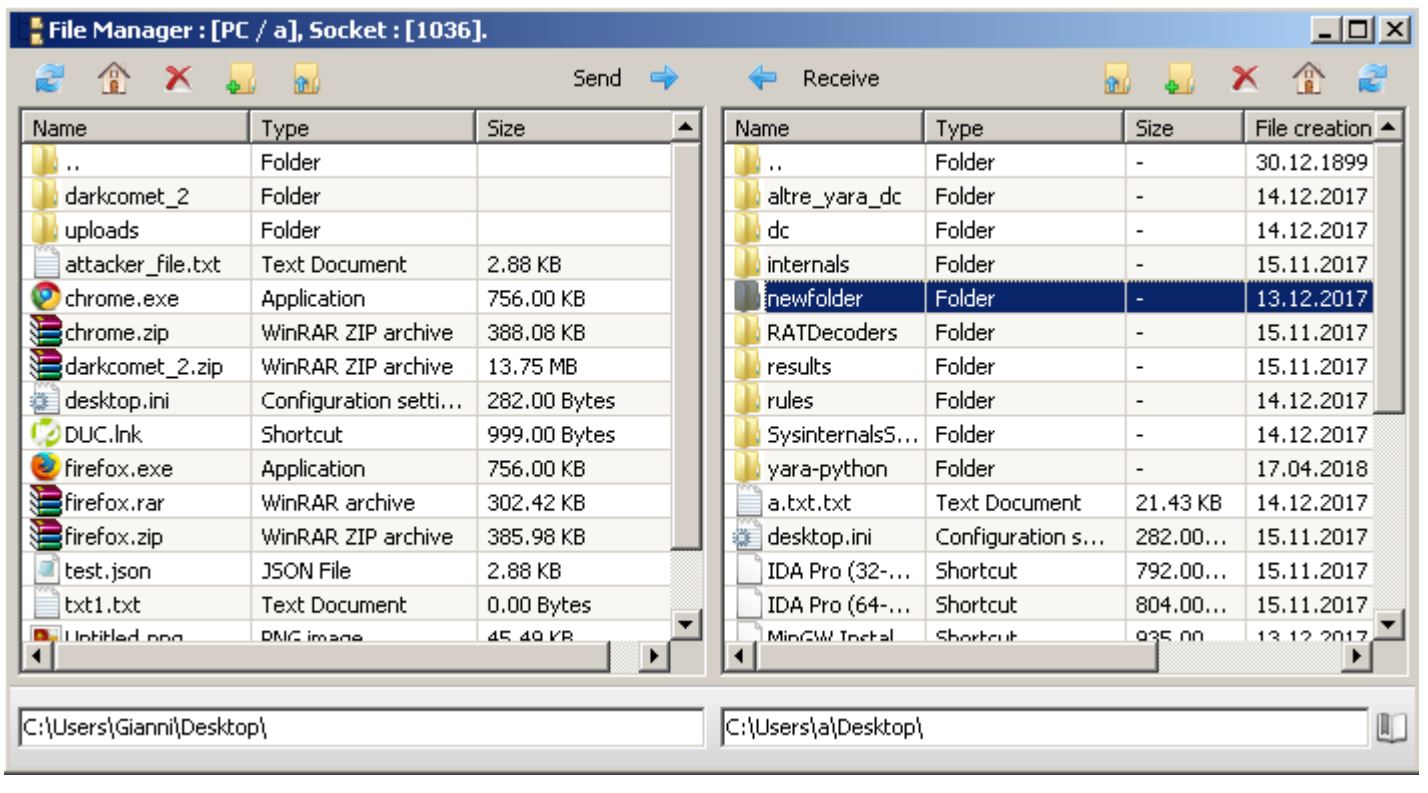
Files Manager -> Explorer Files -> Download





Files Manager -> Explorer Files -> Move on Folders





Files Manager -> Explorer Files -> Upload

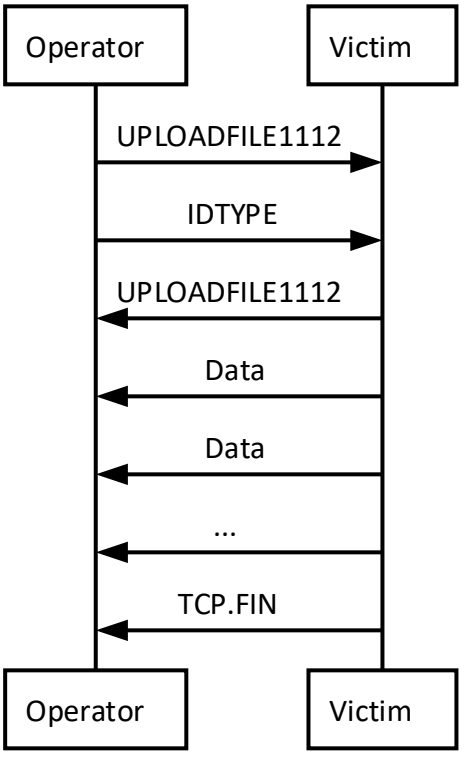
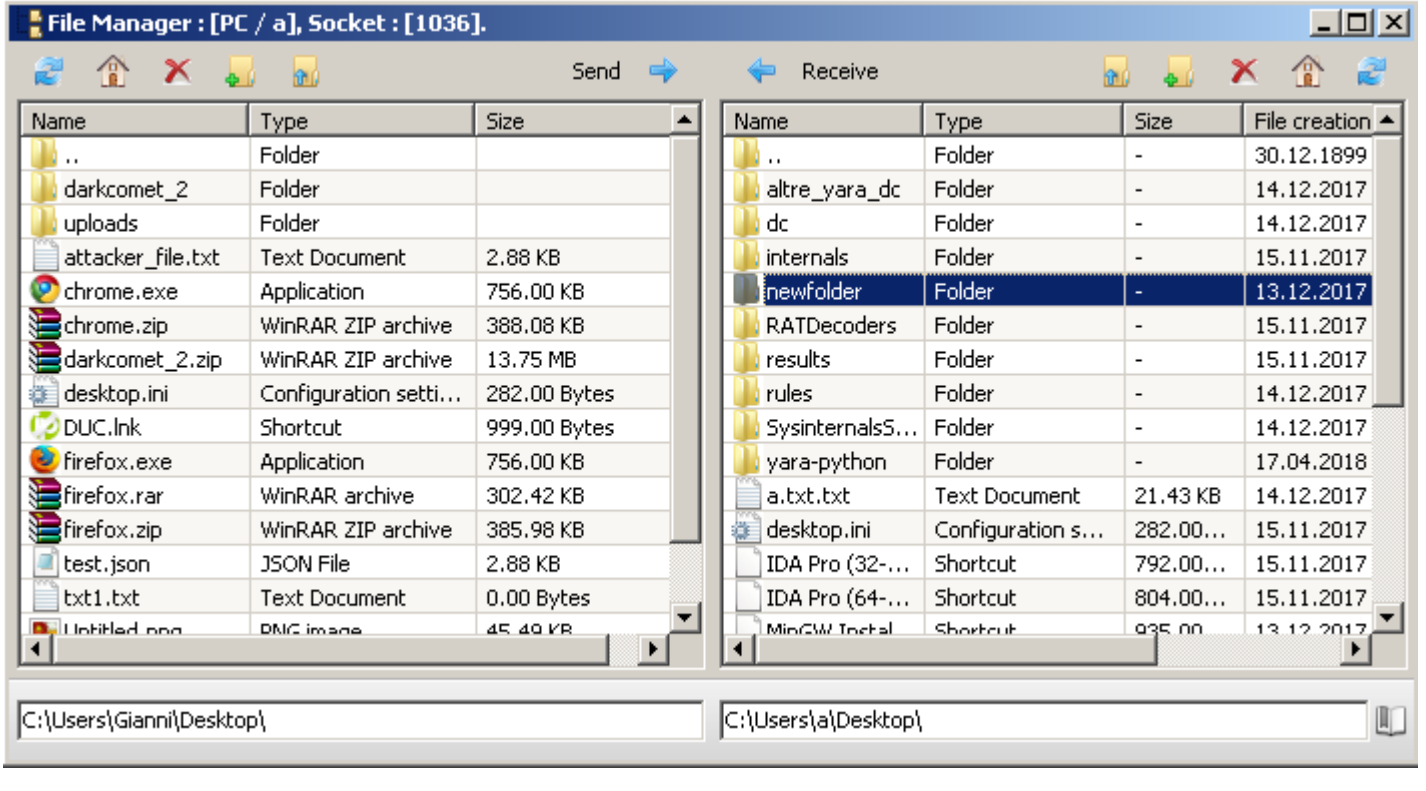
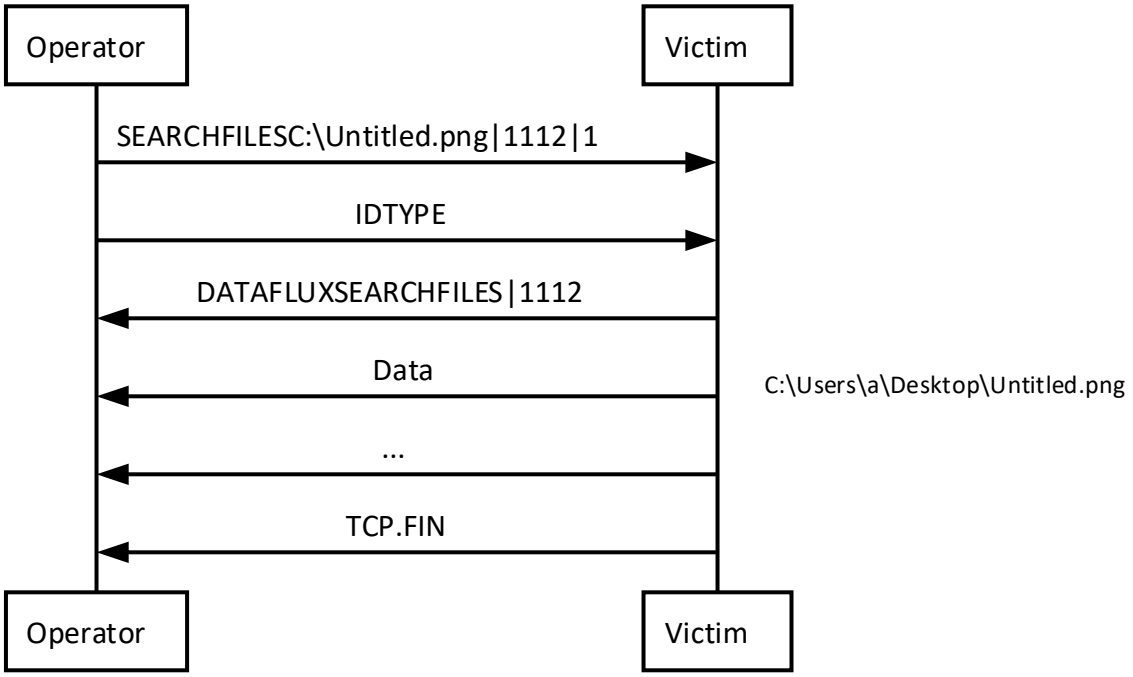
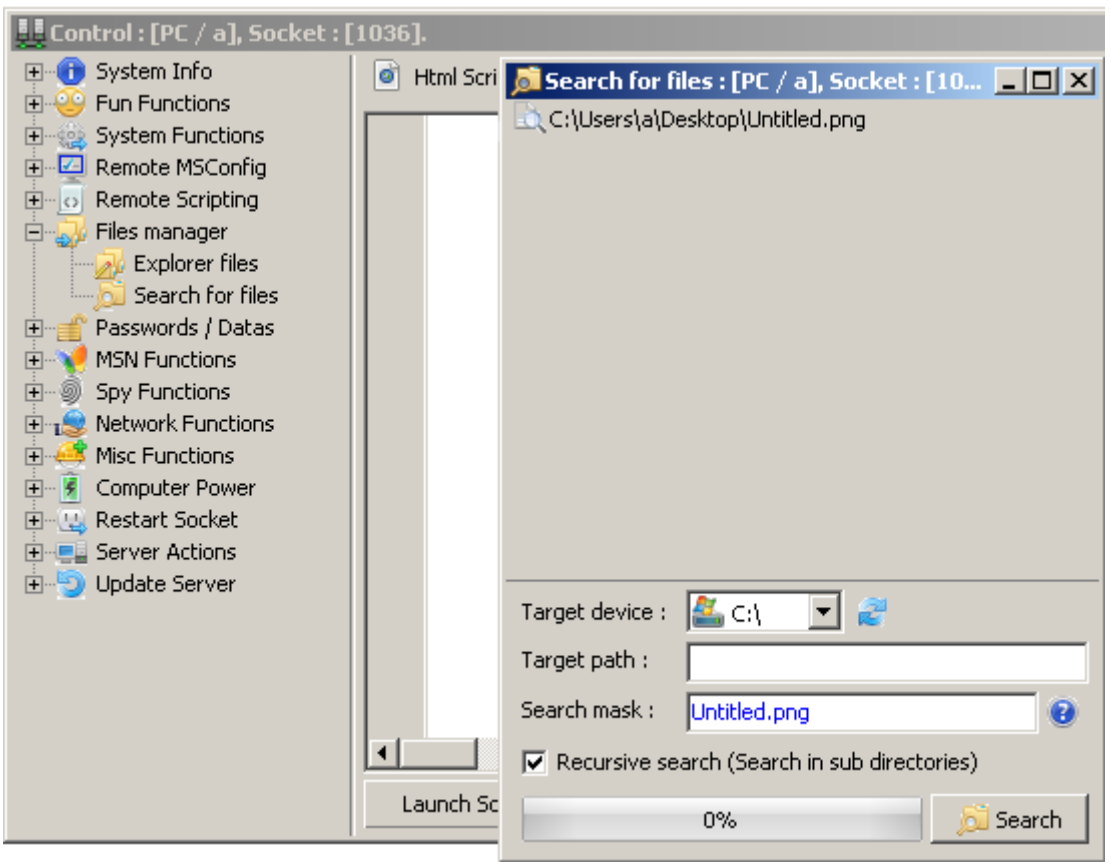


Image is Sent

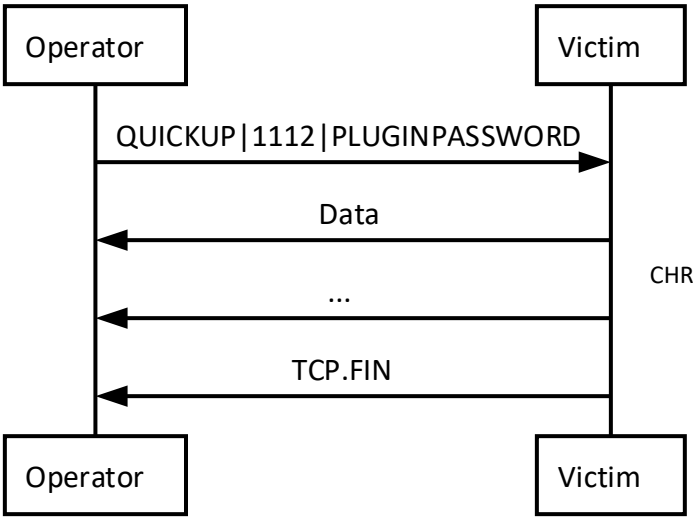


Files Manager -> Search For Files

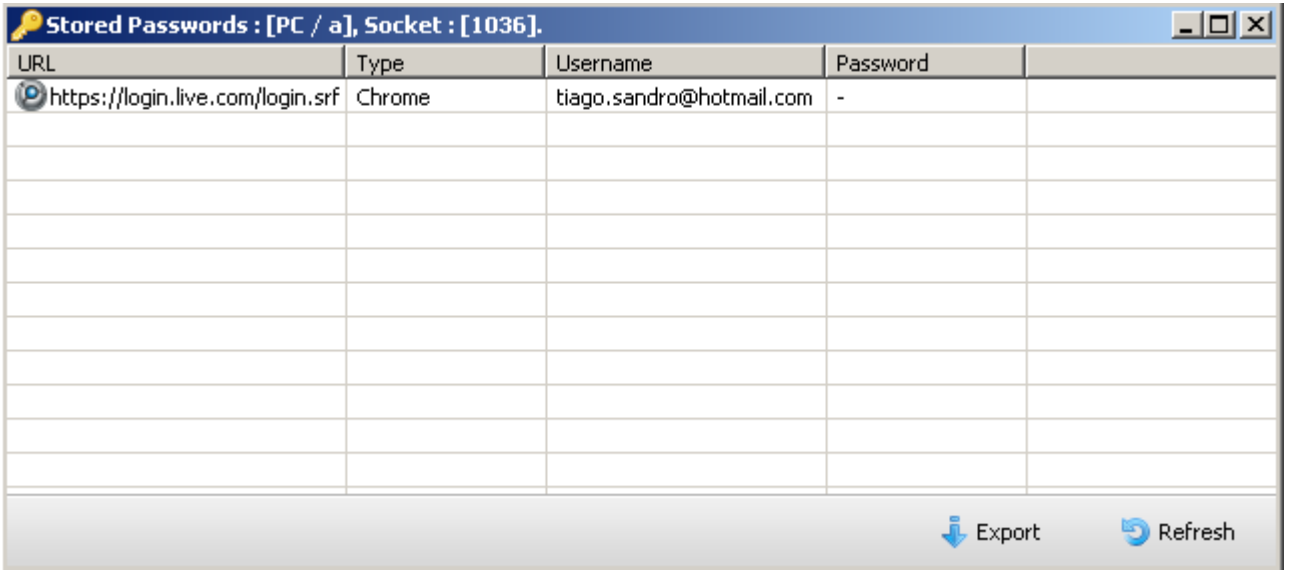




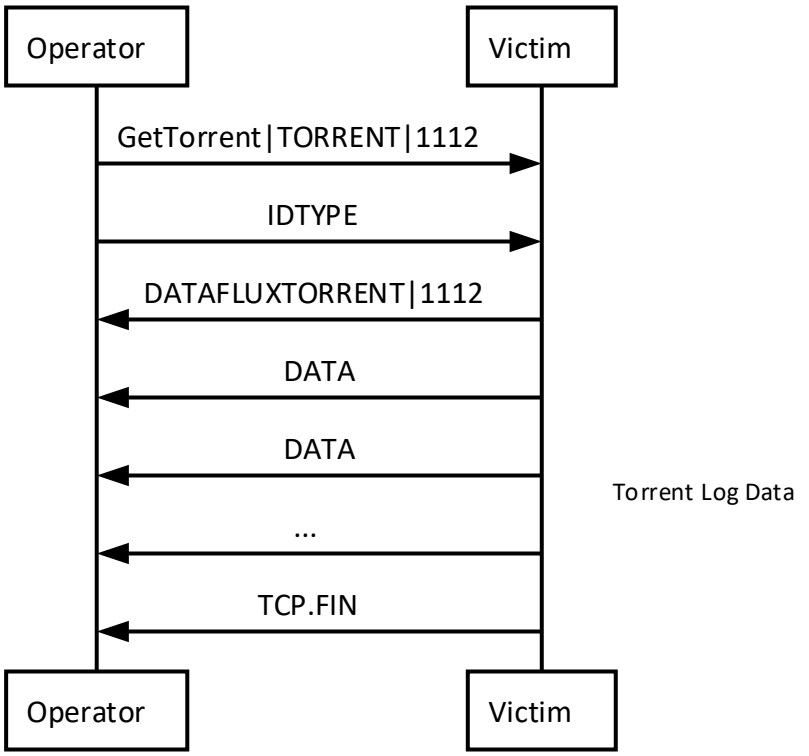
Passwords / Datas -> Stored Passwords

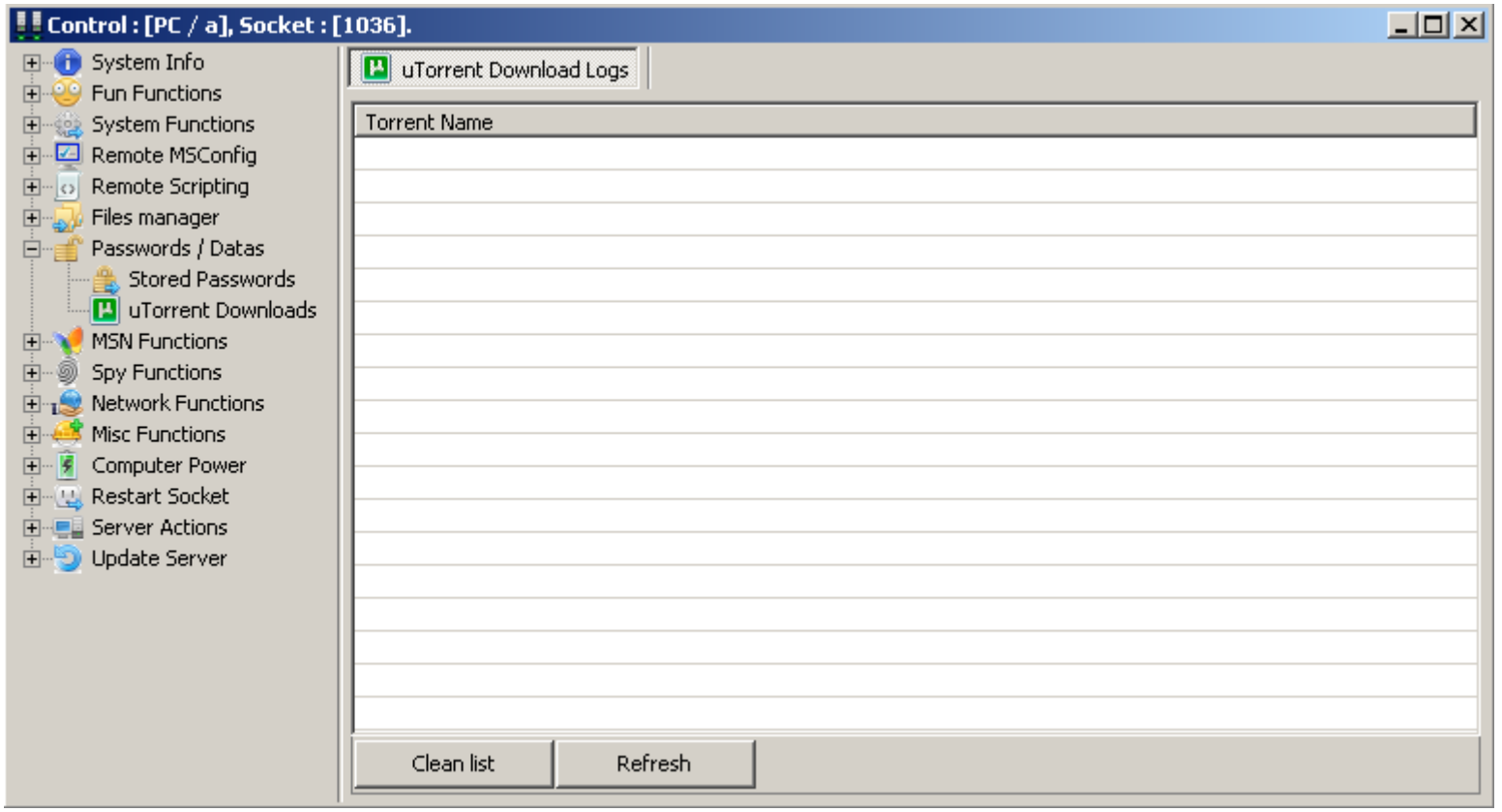


CHR|https://login.live.com/login.srf|tiago.sandro@hotmail.com|-

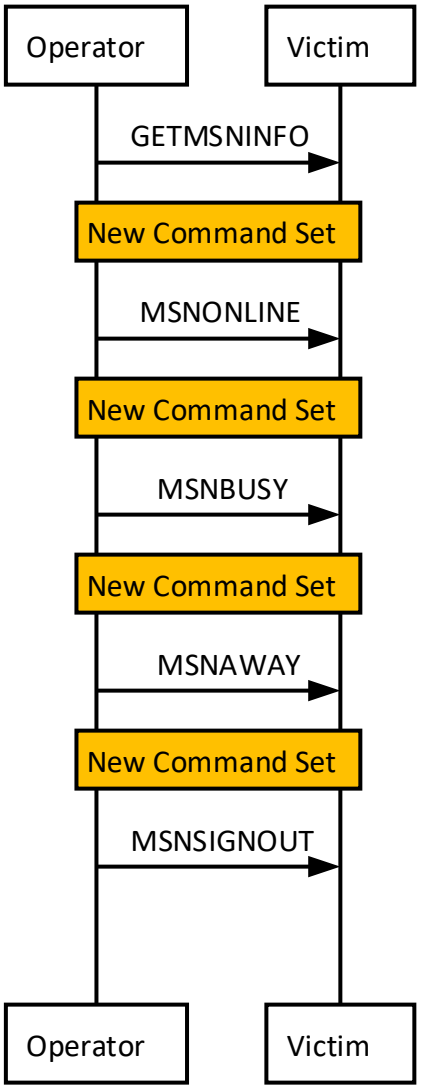


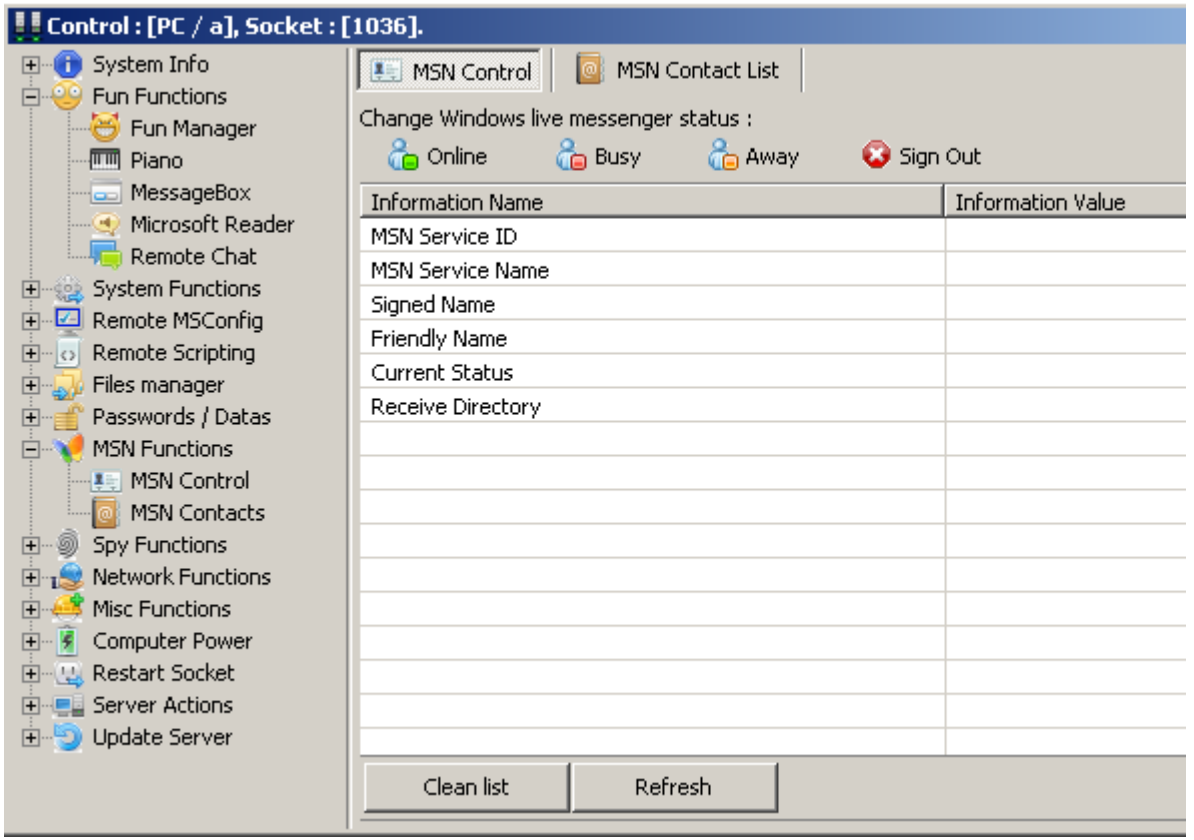
Passwords / Datas -> uTorrent Download Logs



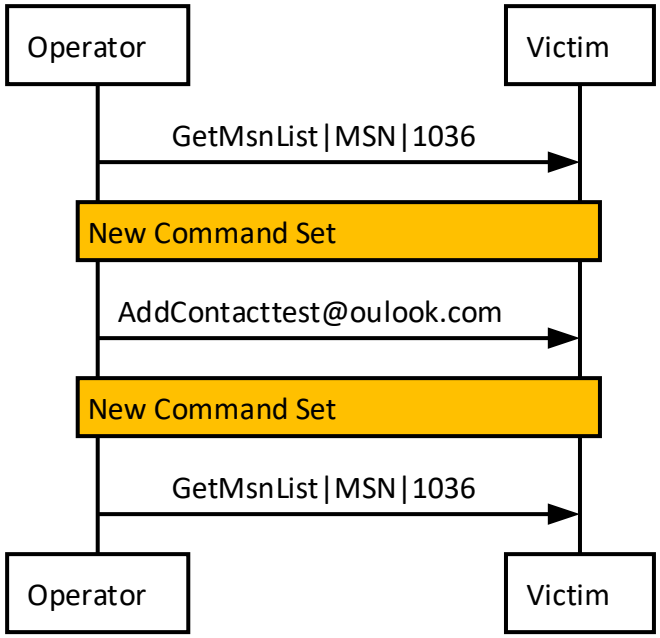


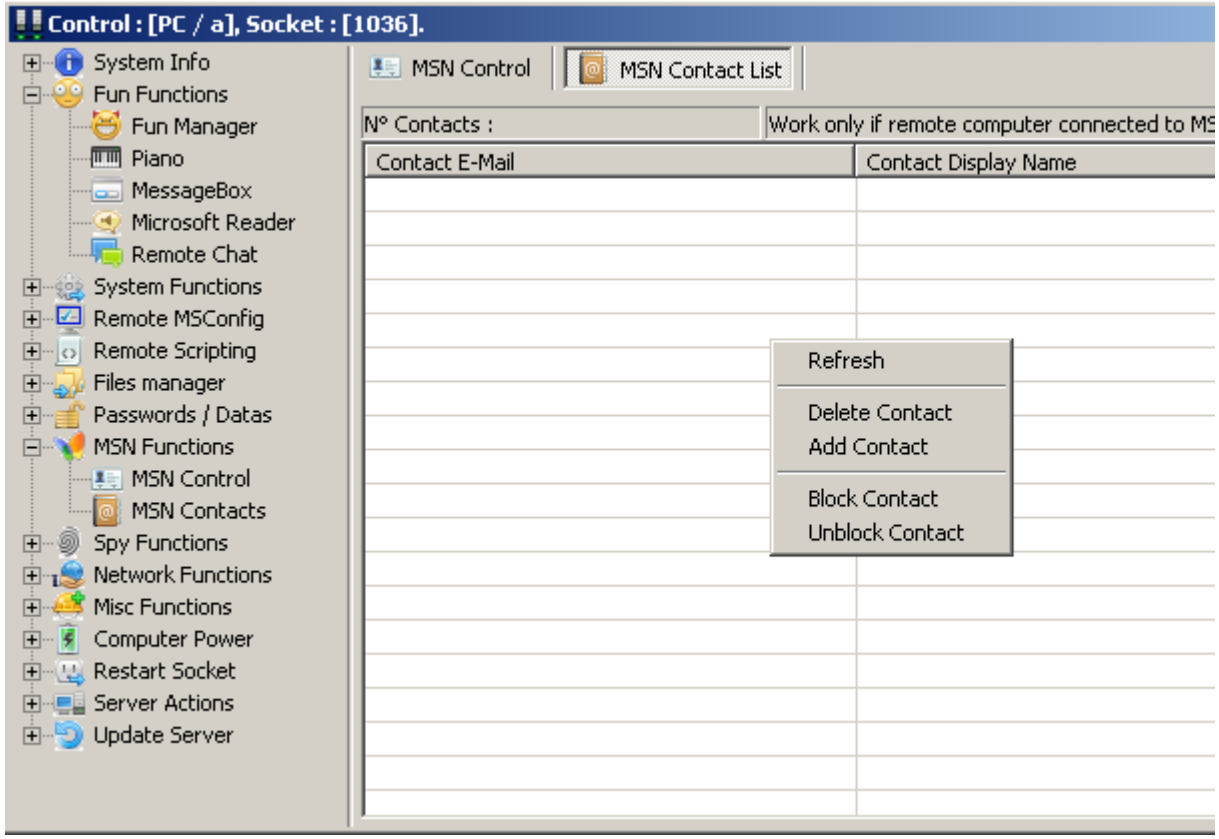
MSN Functions -> MSN Control



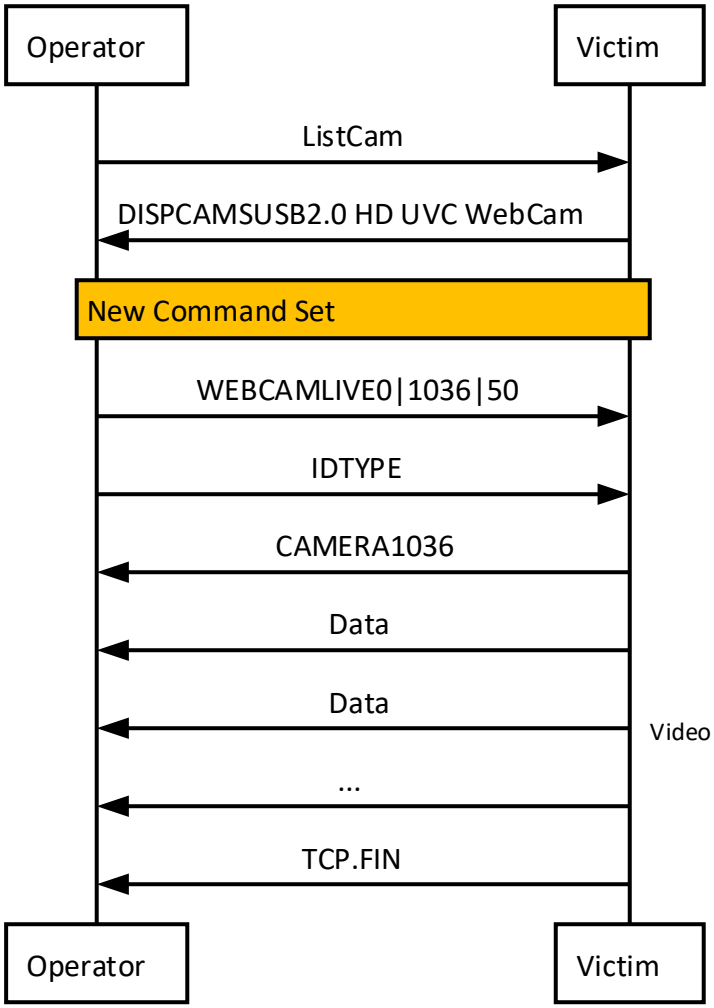


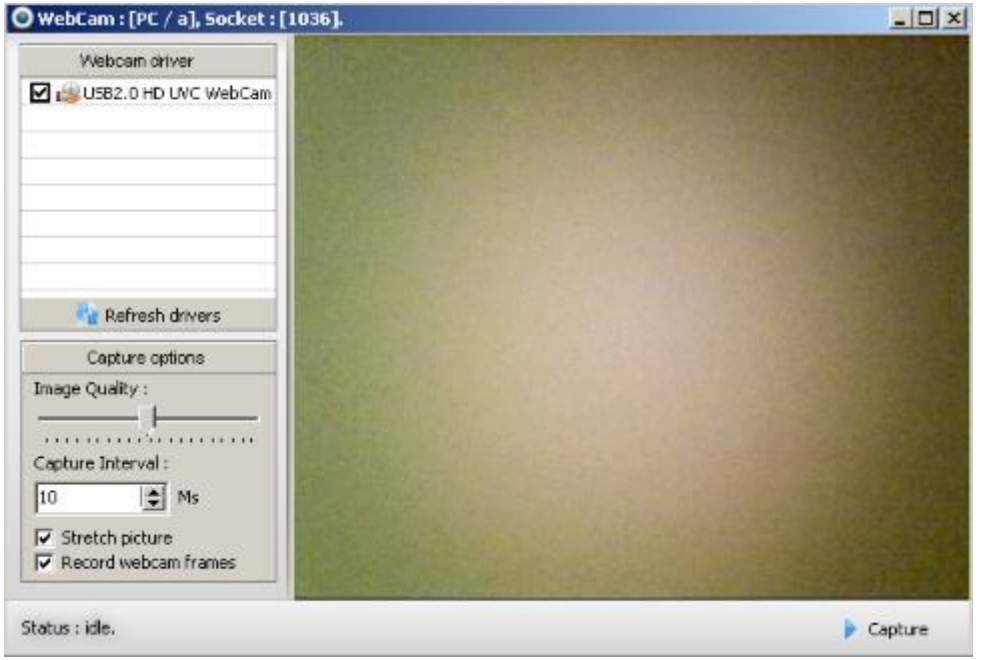
MSN Functions -> MSN Contact List





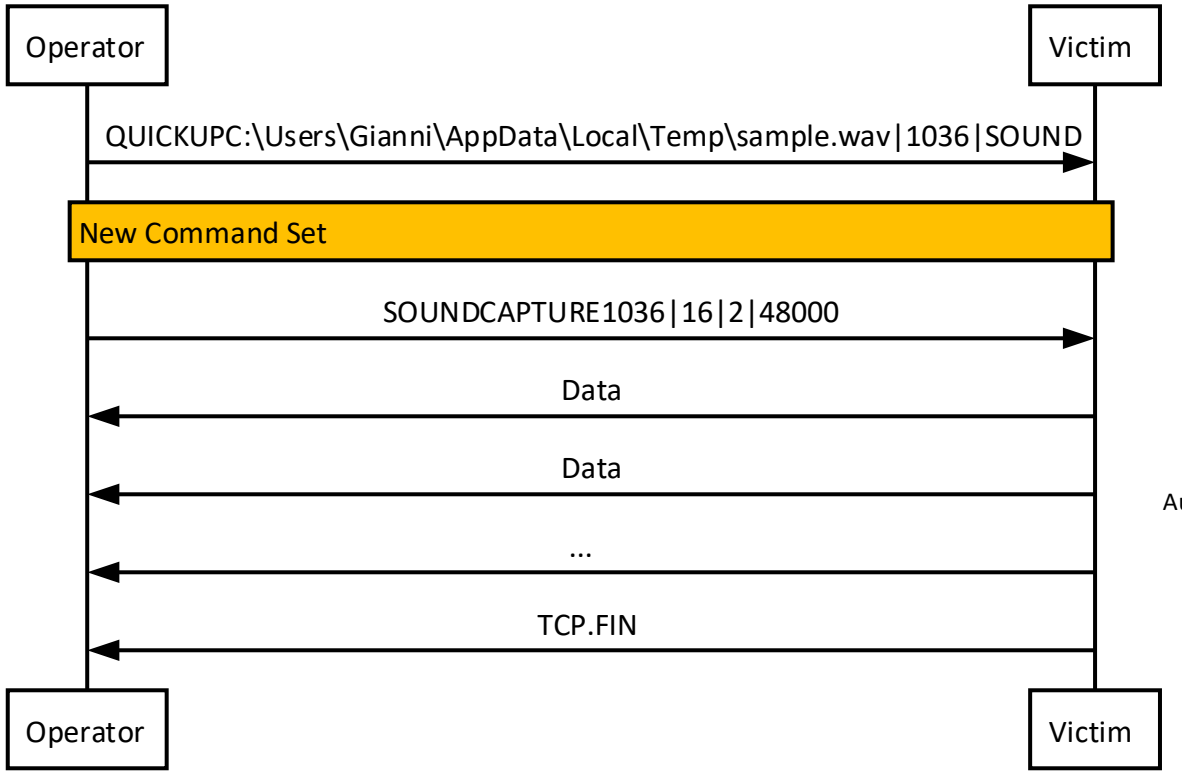
Spy Functions -> Webcam

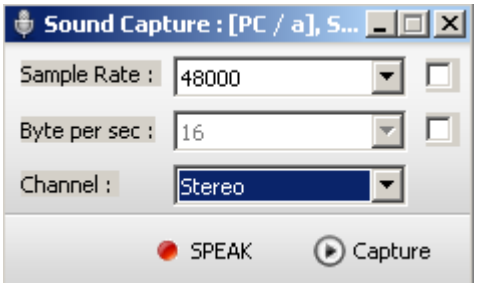




Video Frames are sent

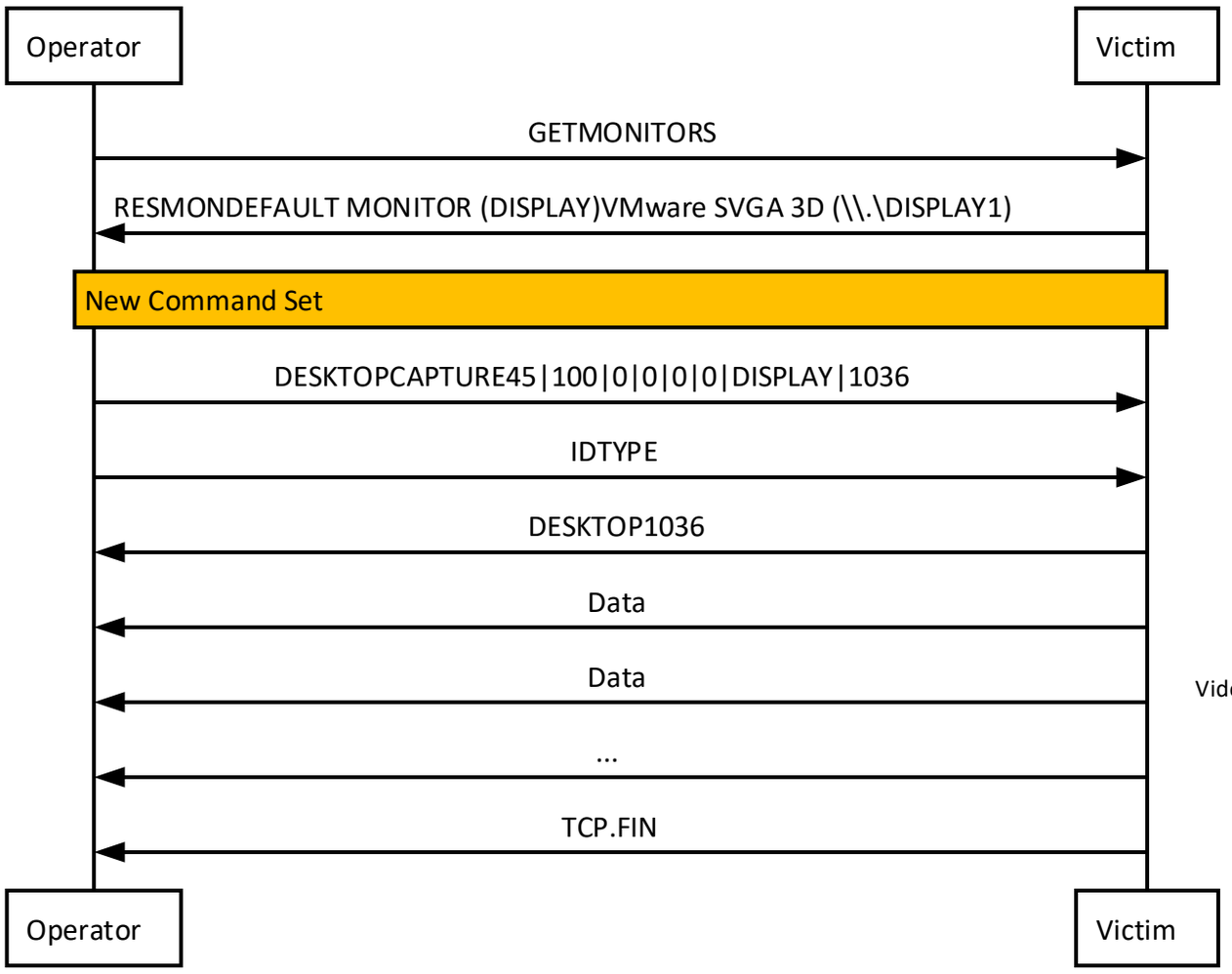
Spy Functions -> Sound Capture



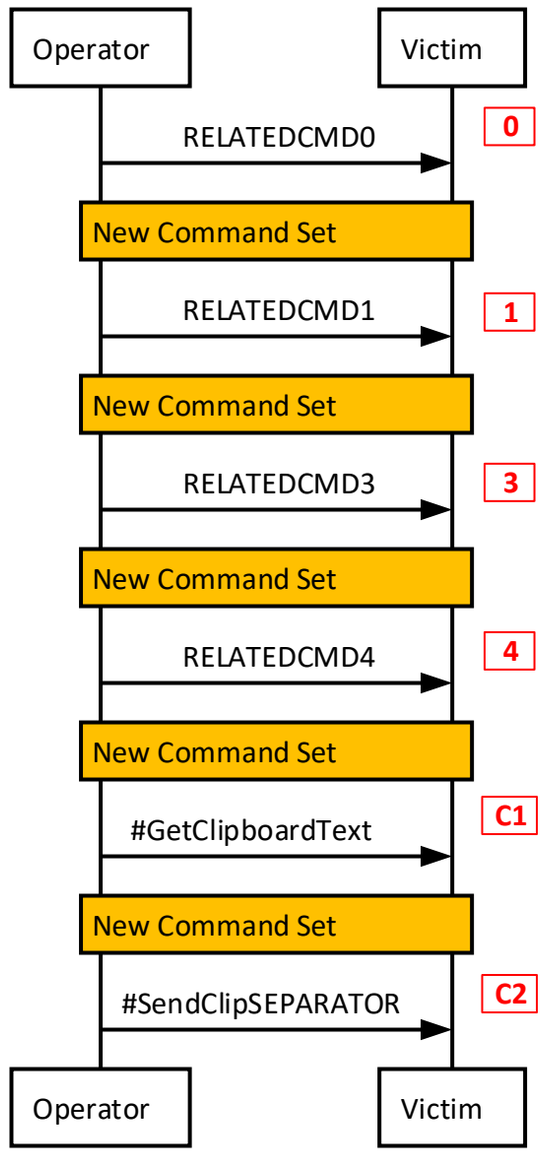


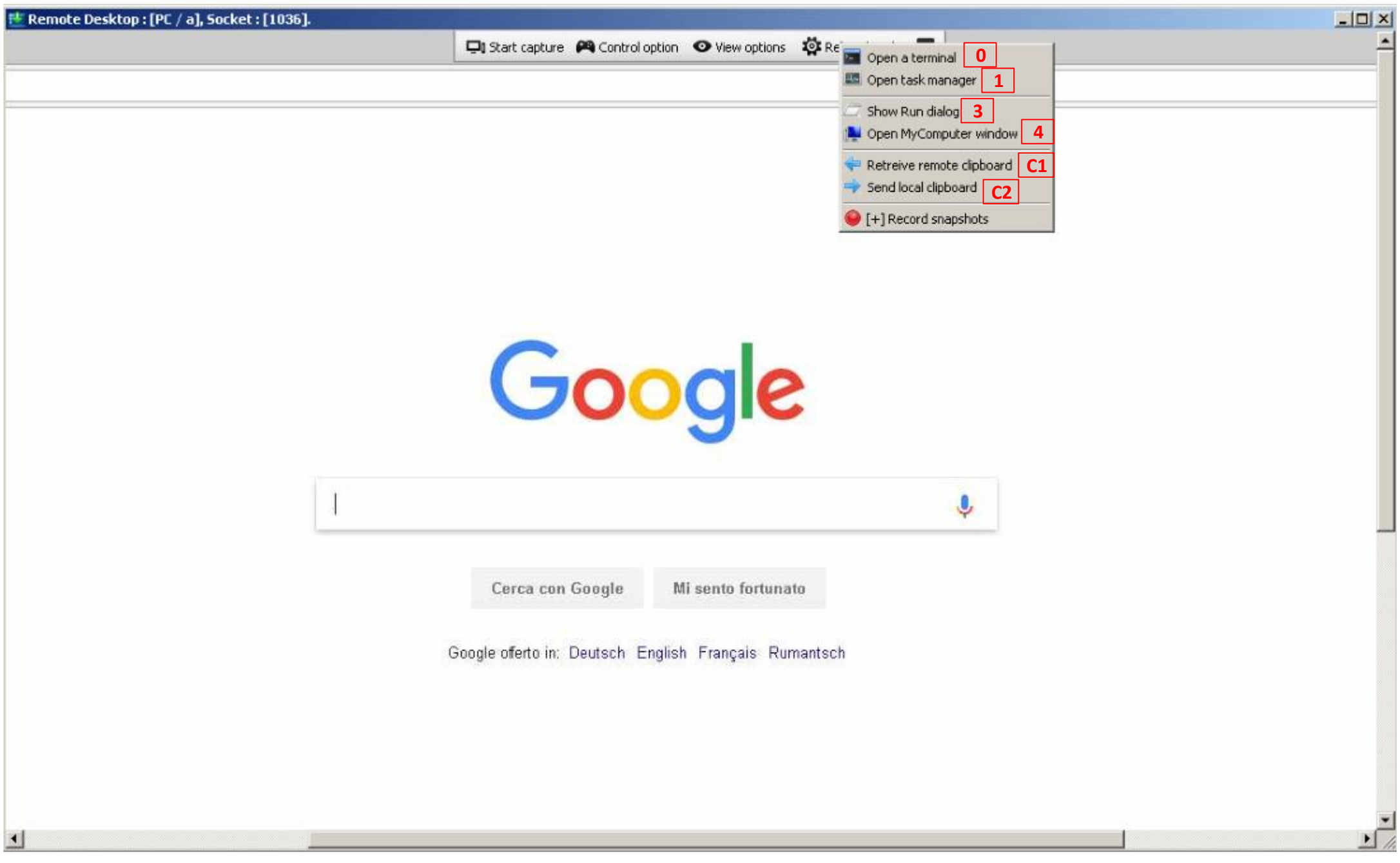
Audio is sent

Spy Functions -> Remote Desktop

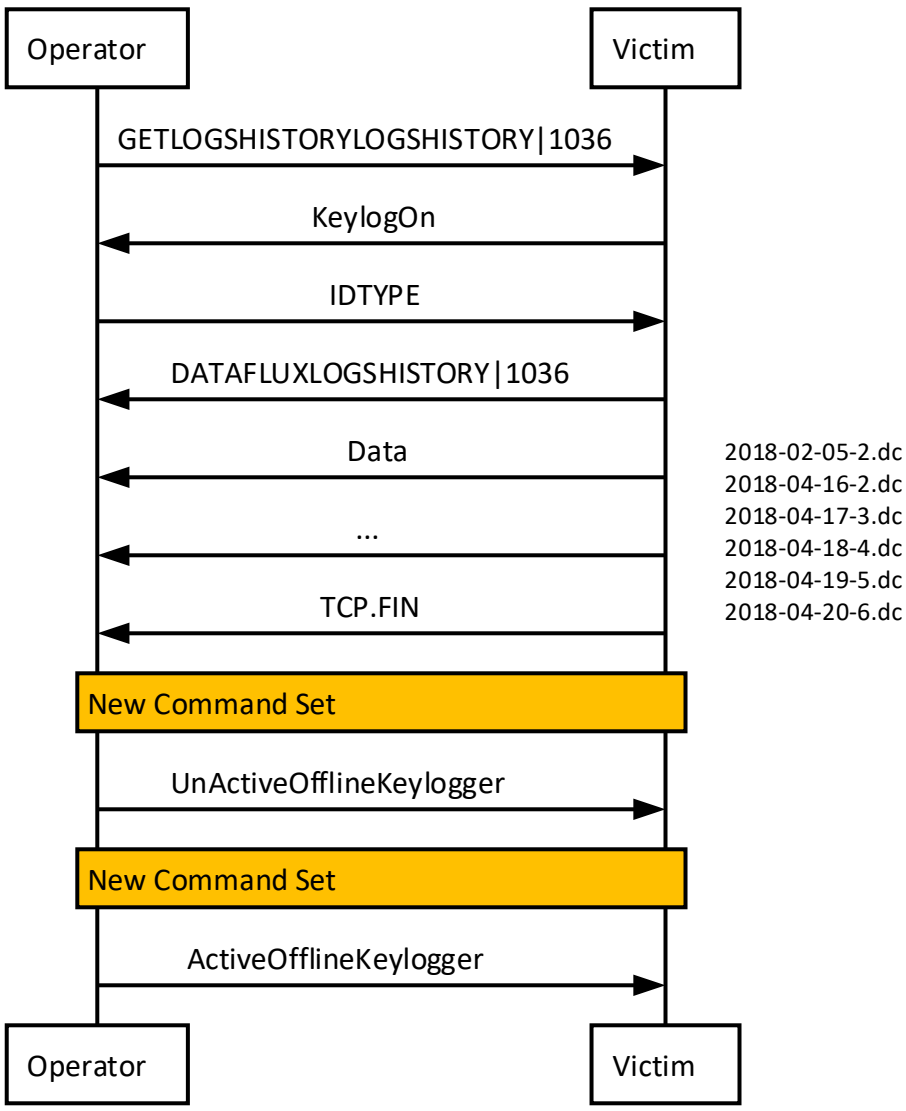


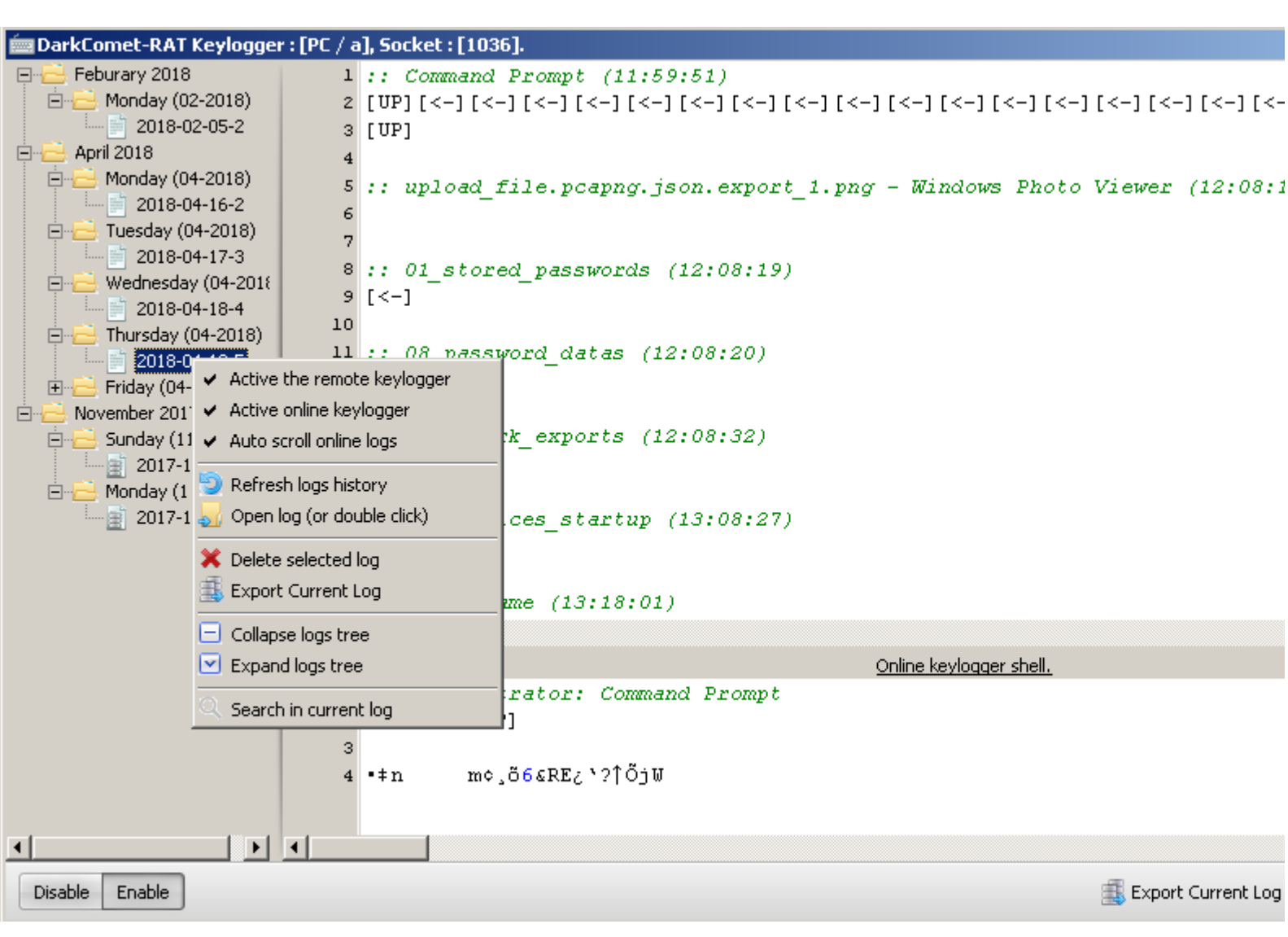
Video is sent



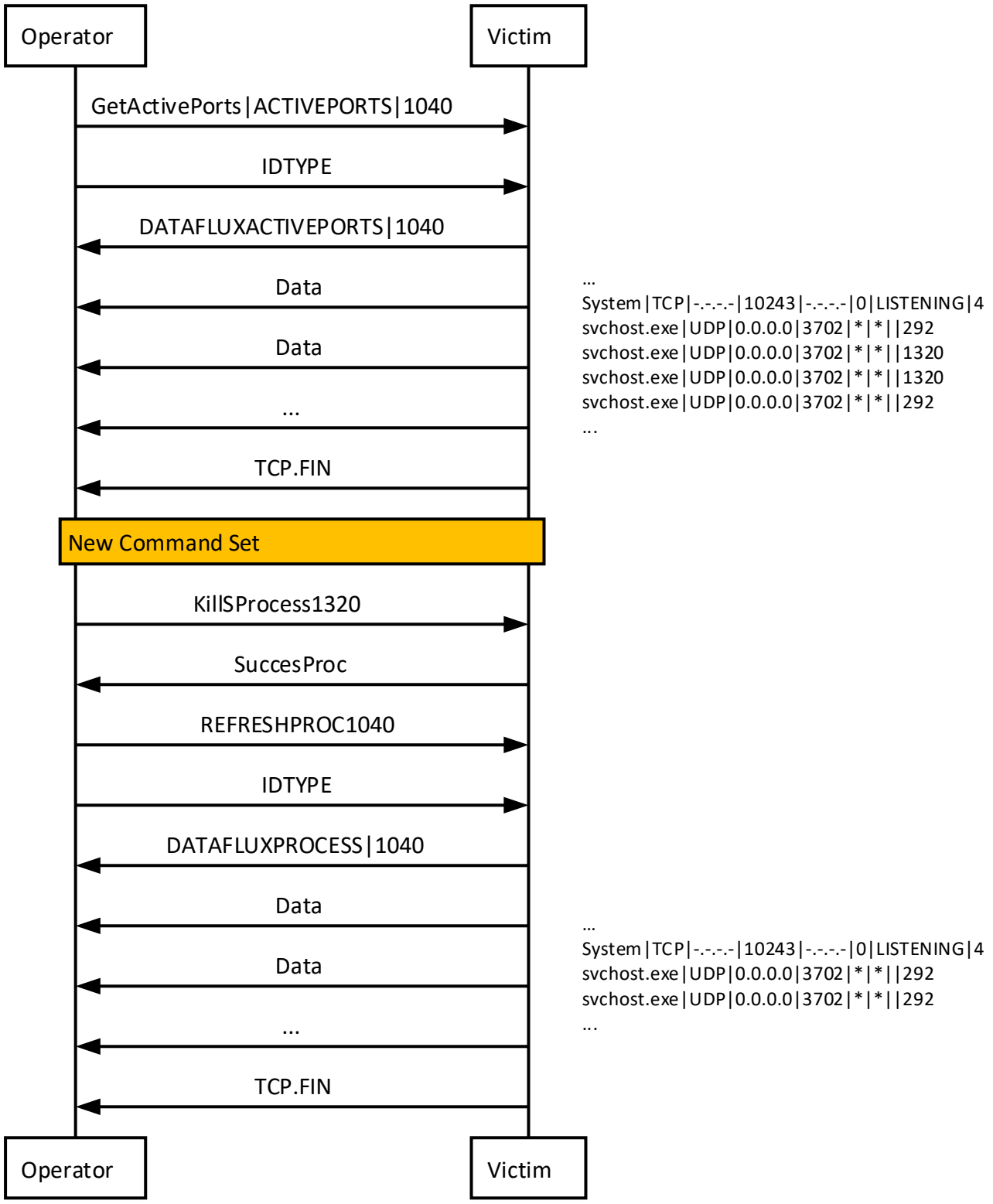


Spy Functions -> Keylogger



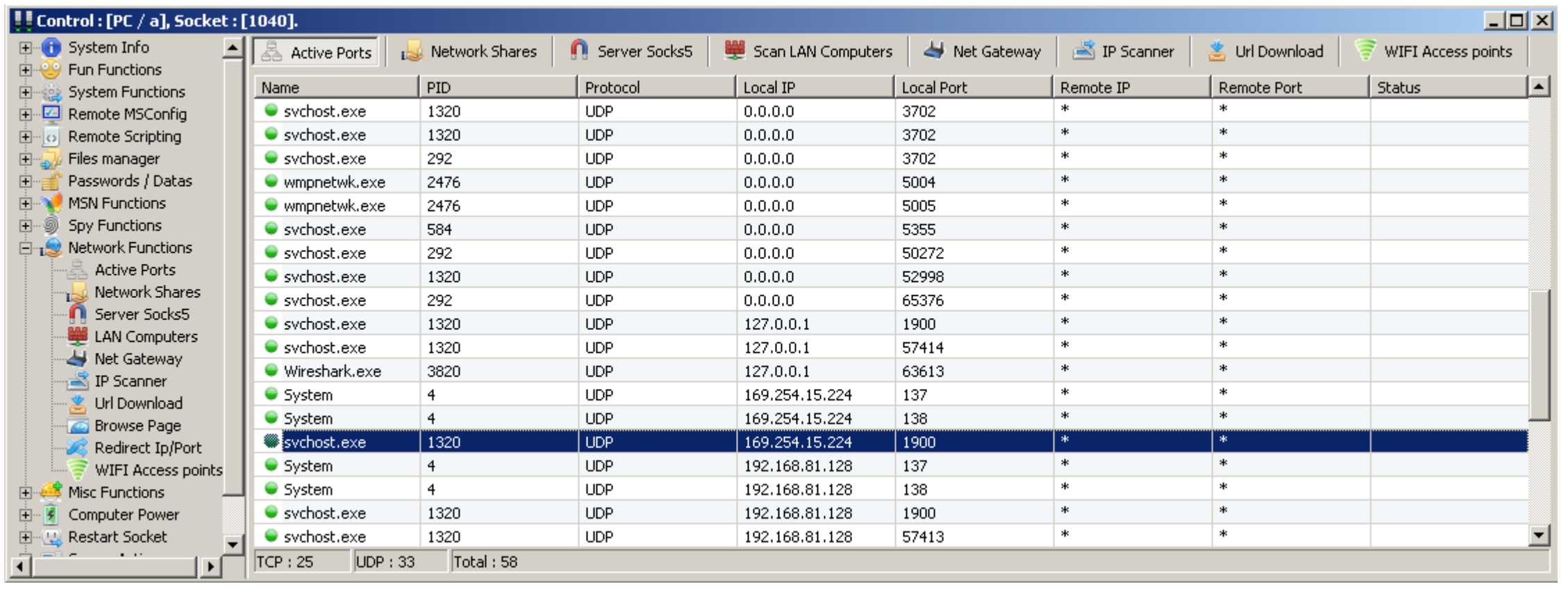


Network Functions -> Active Ports

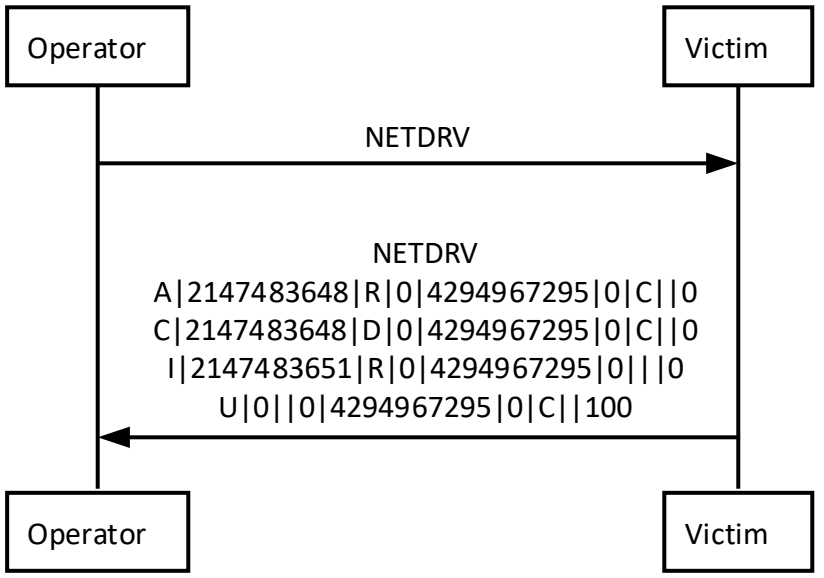


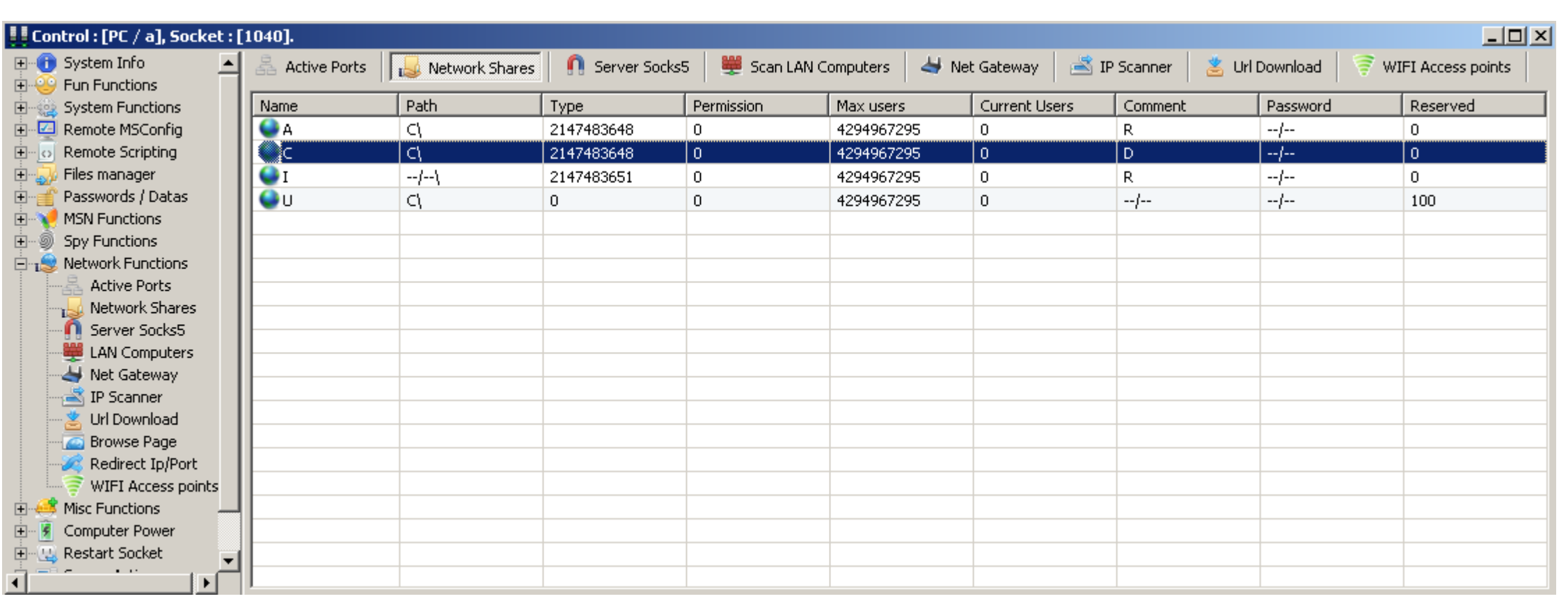

```
...
System|TCP|-.-.-.-|10243|-.-.-.-|0|LISTENING|4
svchost.exe|UDP|0.0.0.0|3702|*|*||292
svchost.exe|UDP|0.0.0.0|3702|*|*||1320
svchost.exe|UDP|0.0.0.0|3702|*|*||1320
svchost.exe|UDP|0.0.0.0|3702|*|*||292
...
```

```
...
System|TCP|-.-.-.-|10243|-.-.-.-|0|LISTENING|4
svchost.exe|UDP|0.0.0.0|3702|*|*||292
svchost.exe|UDP|0.0.0.0|3702|*|*||292
...
```



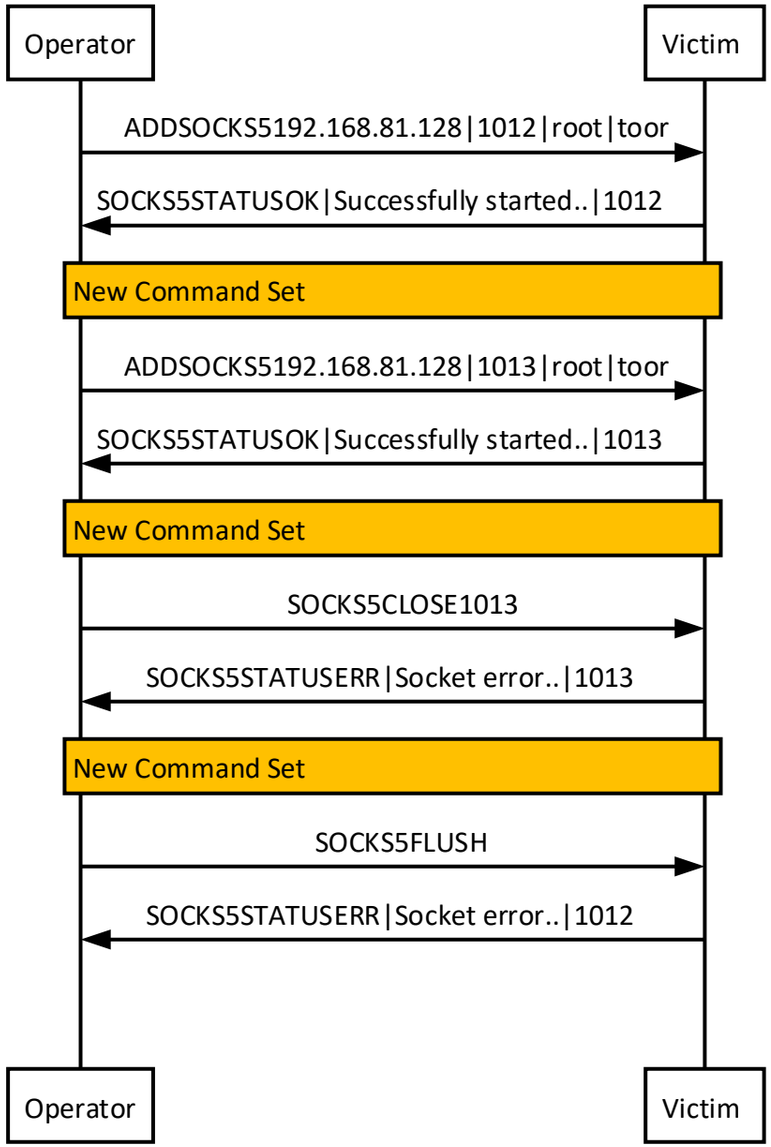
Name	PID	Protocol	Local IP	Local Port	Remote IP	Remote Port	Status
svchost.exe	1320	UDP	0.0.0.0	3702	*	*	
svchost.exe	1320	UDP	0.0.0.0	3702	*	*	
svchost.exe	292	UDP	0.0.0.0	3702	*	*	
wmpnetwk.exe	2476	UDP	0.0.0.0	5004	*	*	
wmpnetwk.exe	2476	UDP	0.0.0.0	5005	*	*	
svchost.exe	584	UDP	0.0.0.0	5355	*	*	
svchost.exe	292	UDP	0.0.0.0	50272	*	*	
svchost.exe	1320	UDP	0.0.0.0	52998	*	*	
svchost.exe	292	UDP	0.0.0.0	65376	*	*	
svchost.exe	1320	UDP	127.0.0.1	1900	*	*	
svchost.exe	1320	UDP	127.0.0.1	57414	*	*	
Wireshark.exe	3820	UDP	127.0.0.1	63613	*	*	
System	4	UDP	169.254.15.224	137	*	*	
System	4	UDP	169.254.15.224	138	*	*	
svchost.exe	1320	UDP	169.254.15.224	1900	*	*	
System	4	UDP	192.168.81.128	137	*	*	
System	4	UDP	192.168.81.128	138	*	*	
svchost.exe	1320	UDP	192.168.81.128	1900	*	*	
svchost.exe	1320	UDP	192.168.81.128	57413	*	*	

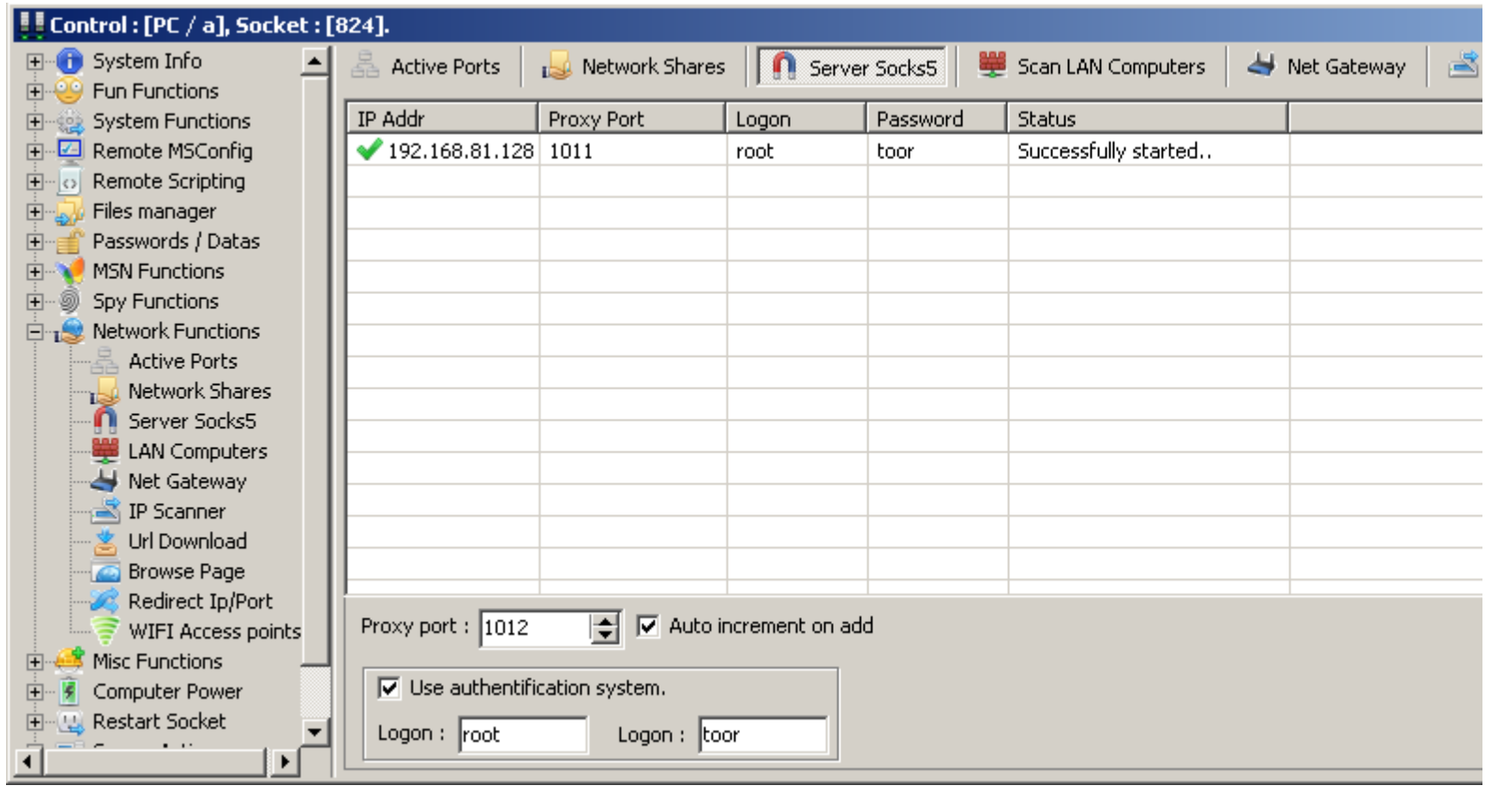




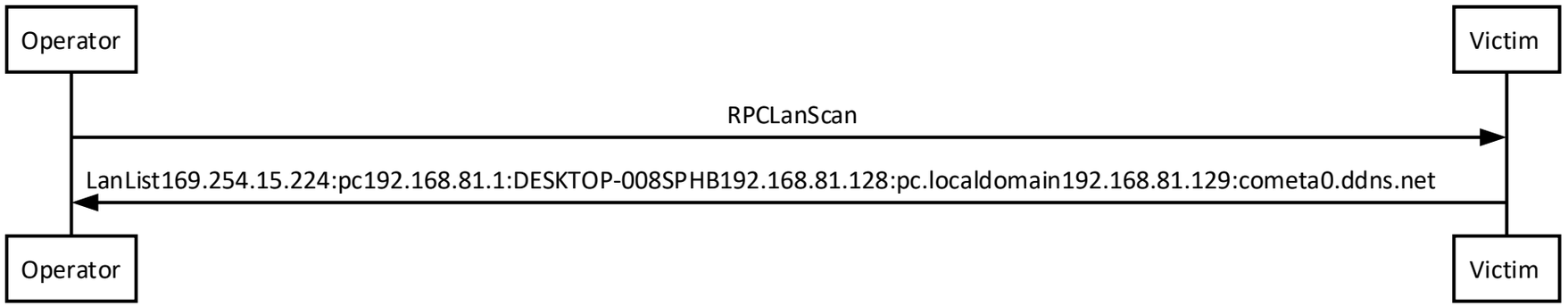
Name	Path	Type	Permission	Max users	Current Users	Comment	Password	Reserved
A	C\	2147483648	0	4294967295	0	R	--/--	0
C	C\	2147483648	0	4294967295	0	D	--/--	0
I	--/--\	2147483651	0	4294967295	0	R	--/--	0
U	C\	0	0	4294967295	0	--/--	--/--	100

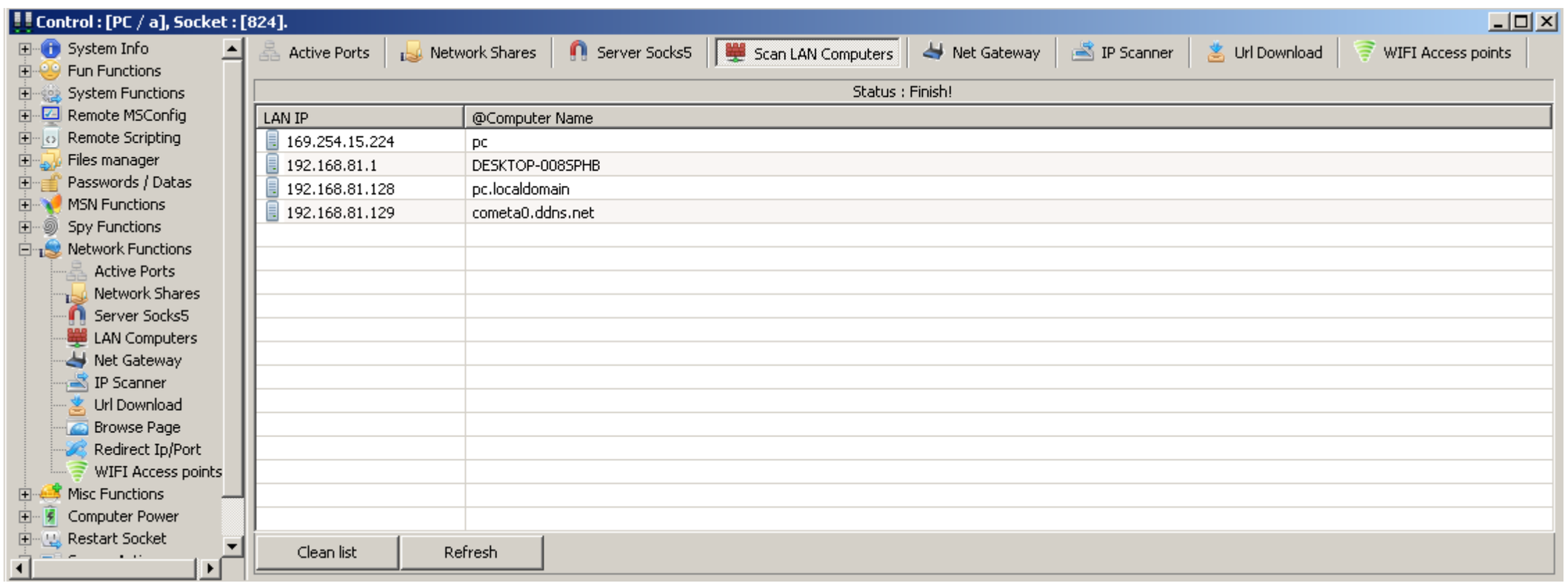
Network Functions -> Server Sockets



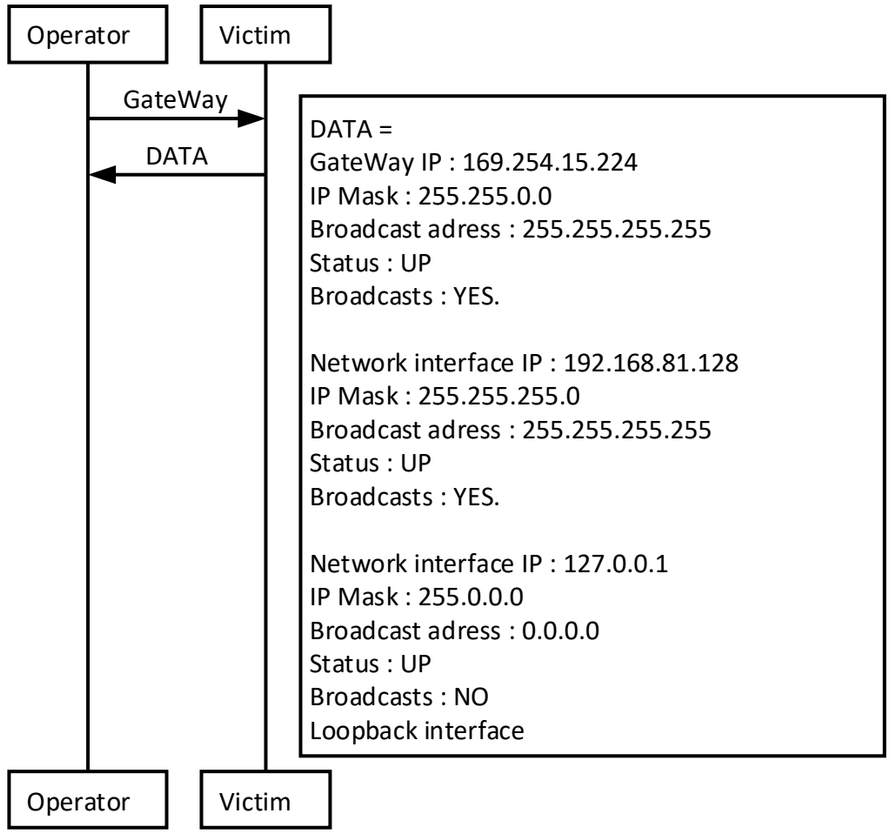


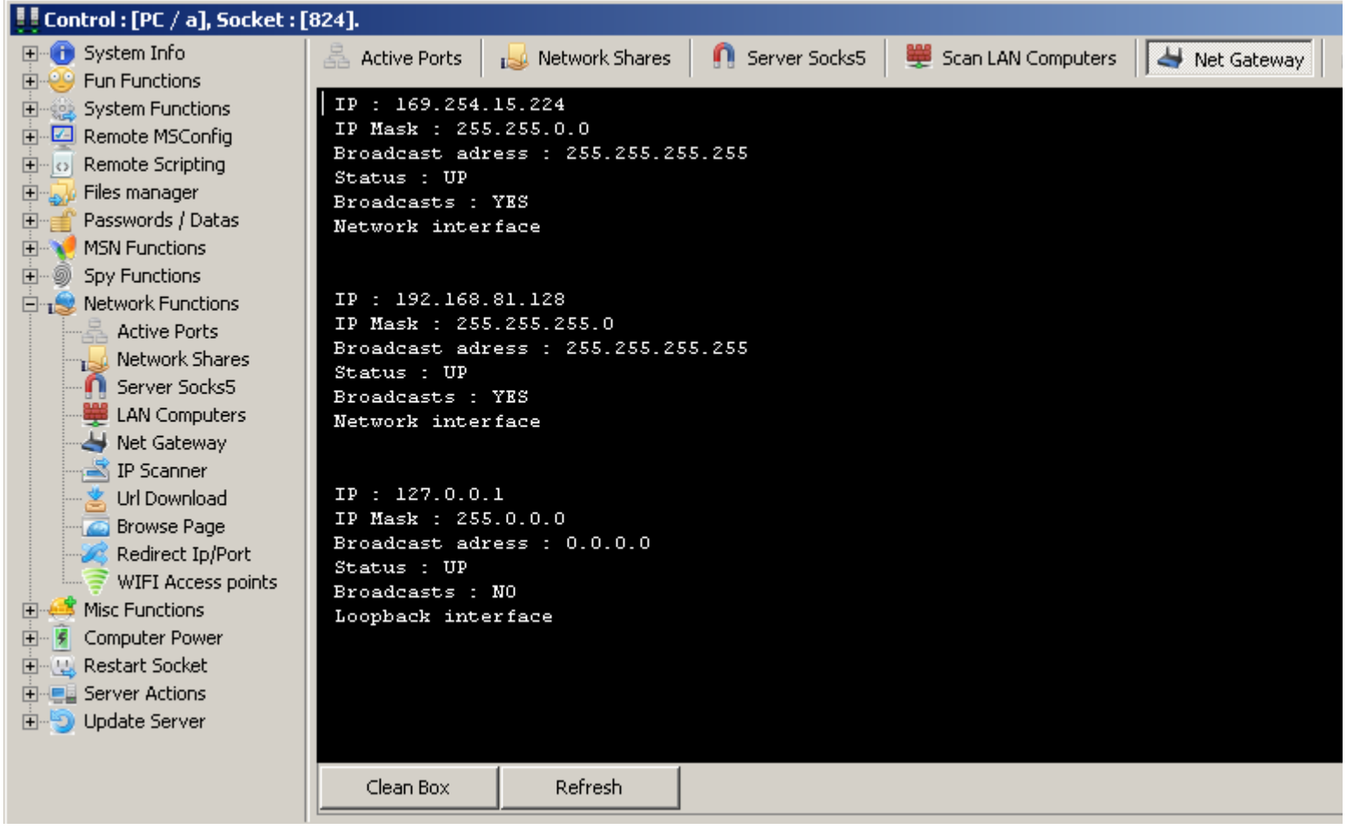
Network Functions -> Scan LAN Computers



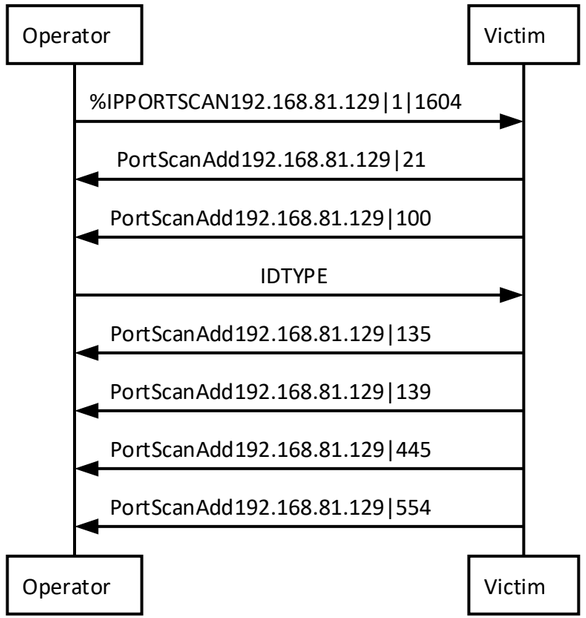


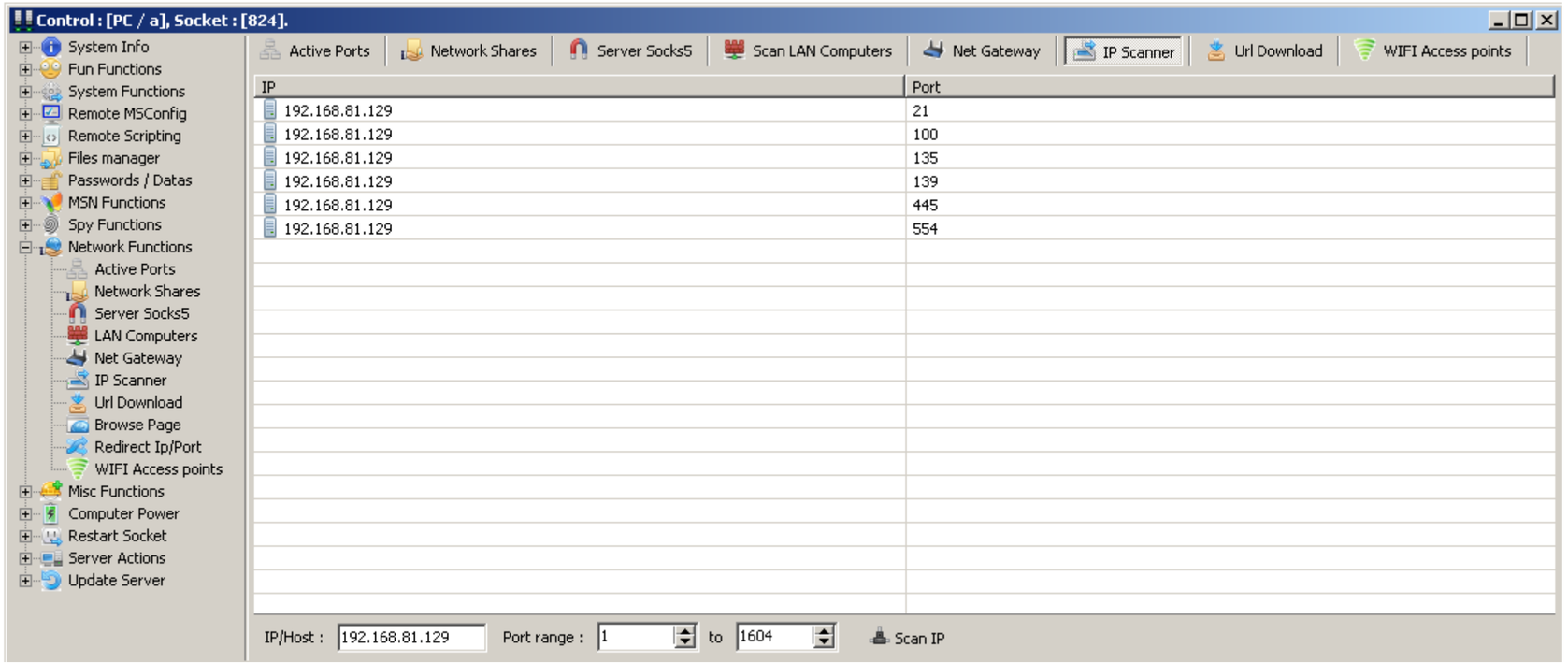
Network Functions -> Net Gateway



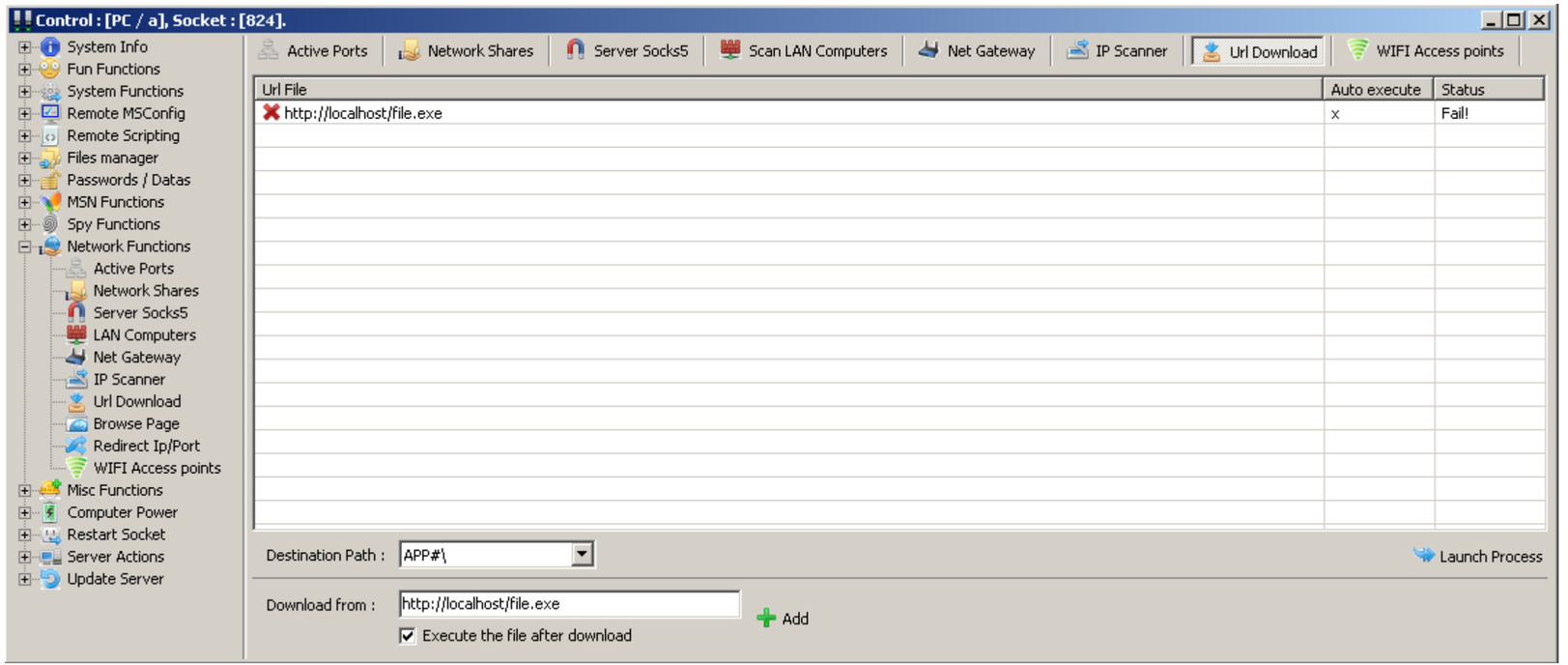


Network Functions -> IP Scanner

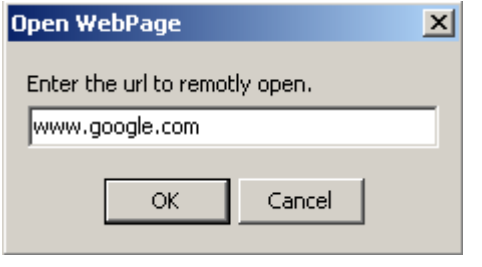




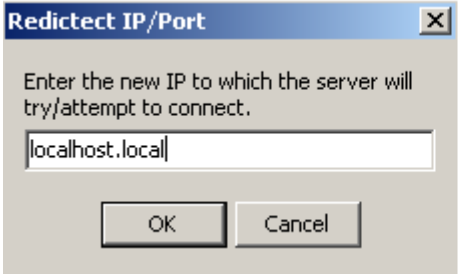
Network Functions -> Url Download

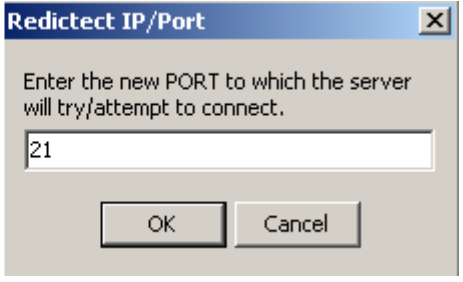


Network Functions -> Browse Page

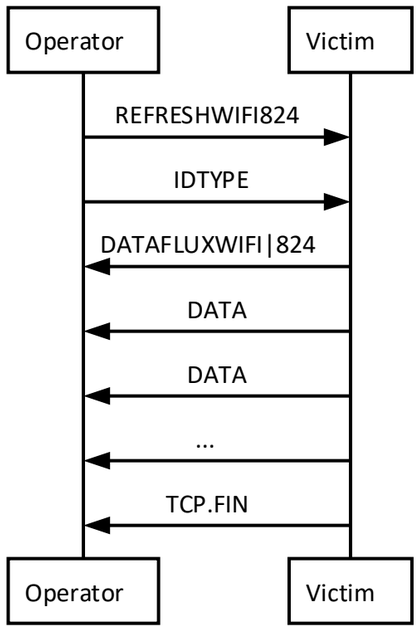


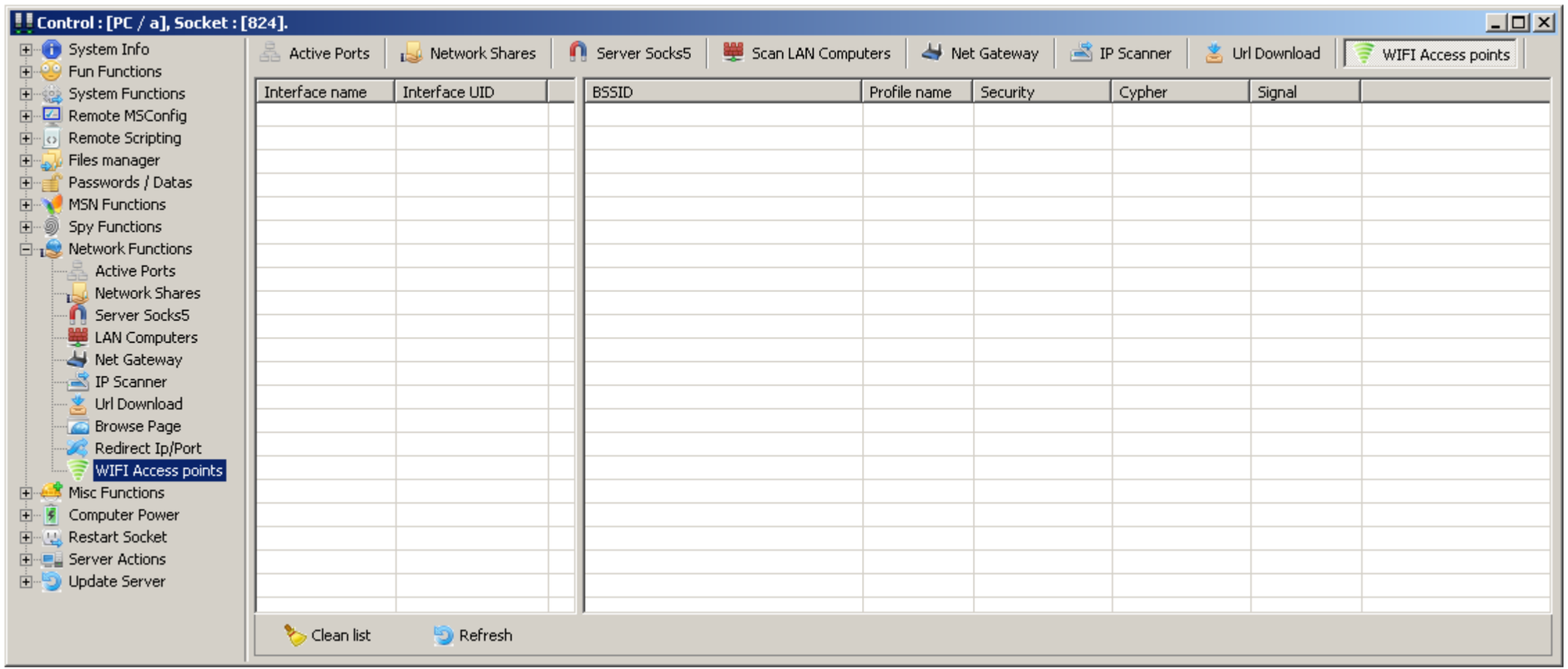
Network Functions -> Redirect IP/Port



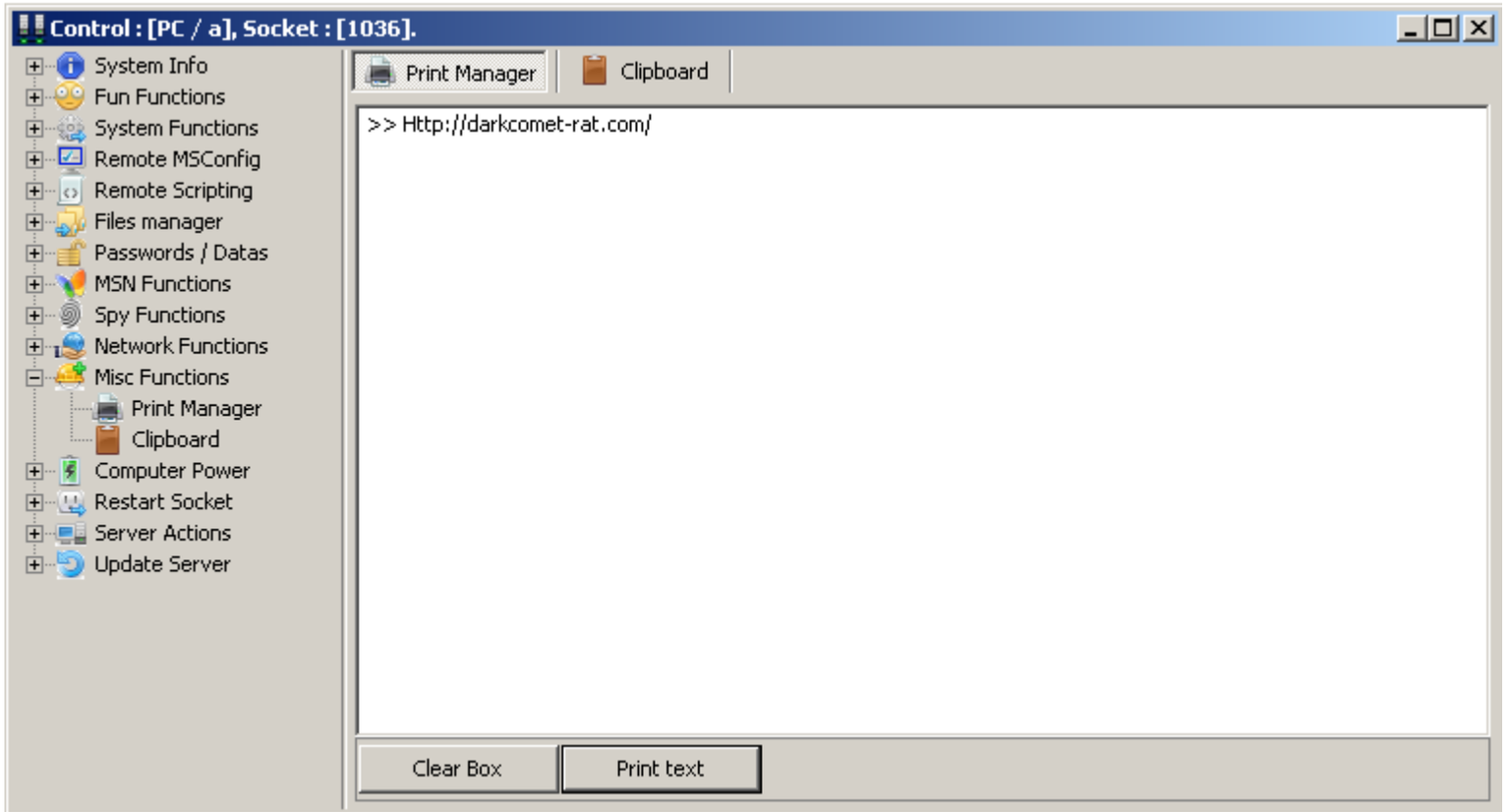


Network Functions -> WiFi Access Points

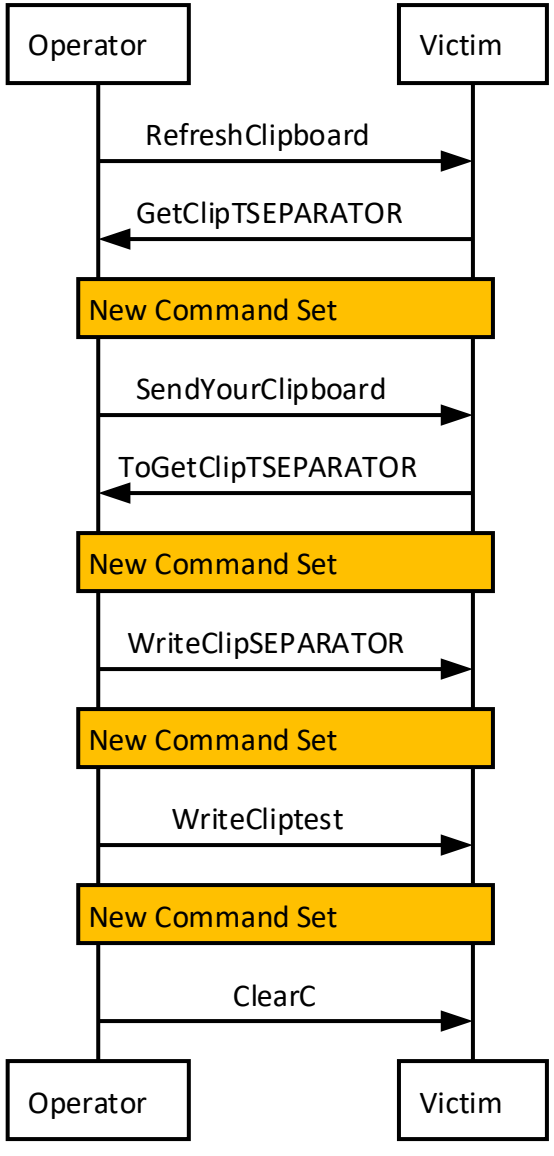


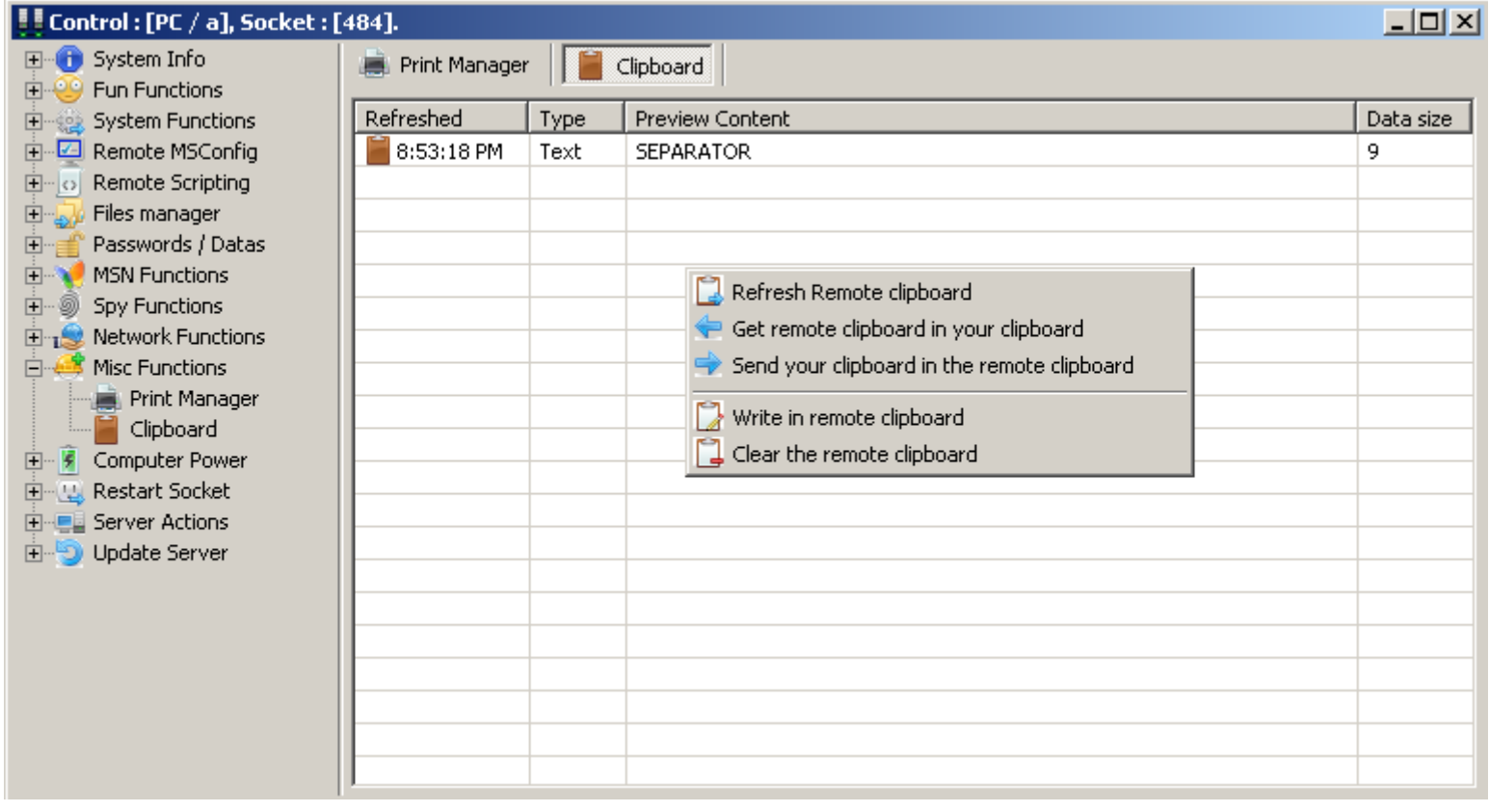


Misc Functions -> Print Manager

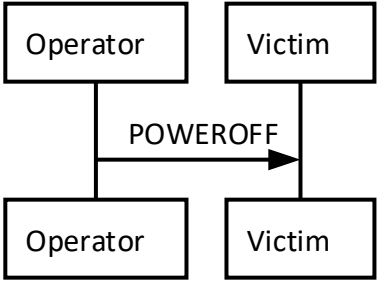


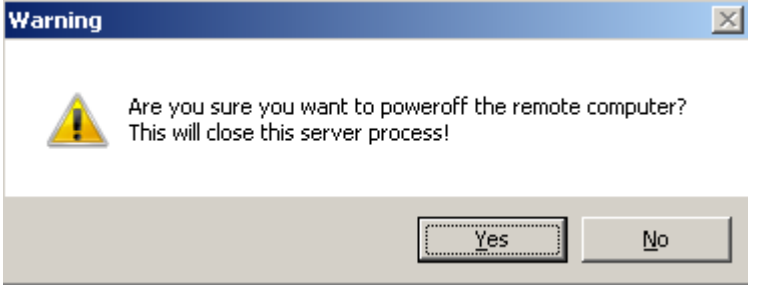
Misc Functions -> Clipboard



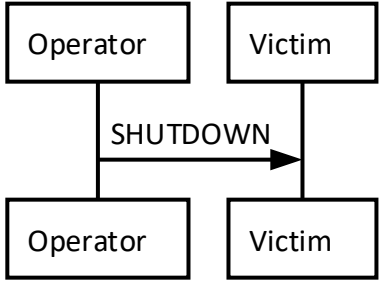


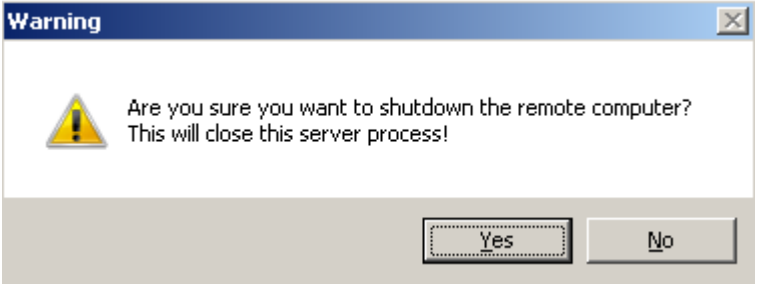
Computer Power -> Poweroff



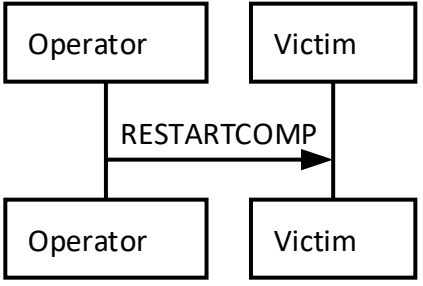


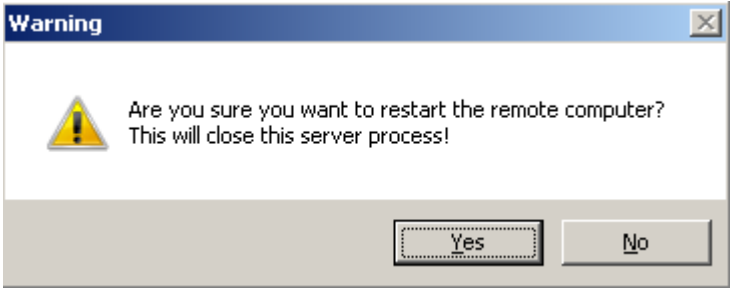
Computer Power -> Shutdown



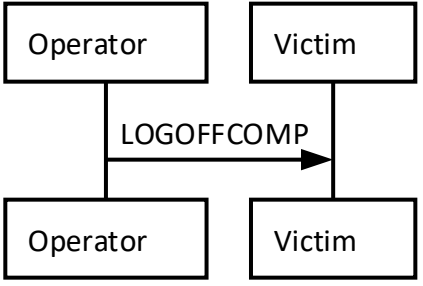


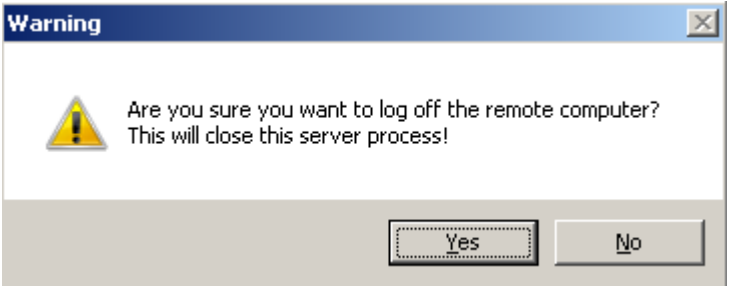
Computer Power -> Restart



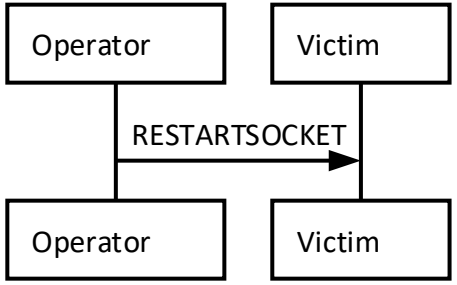


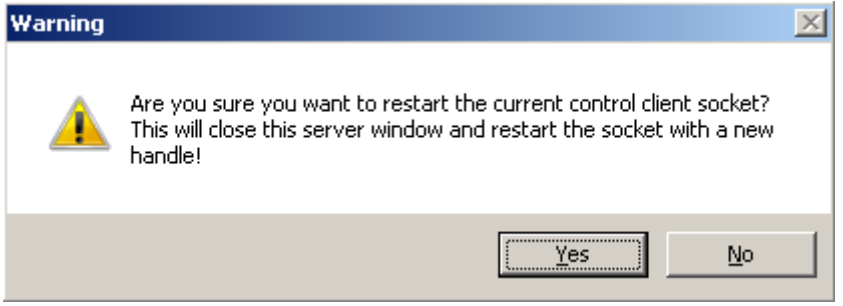
Computer Power -> Logoff





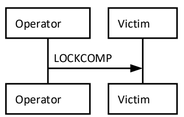
Restart Socket -> Server (Victim)



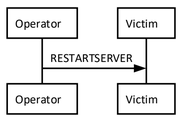


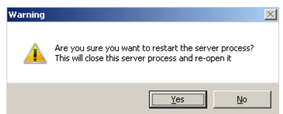
Server Actions

Server Actions -> Lock computer

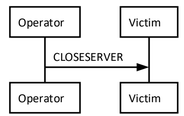


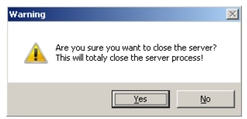
Server Actions -> Restart Server



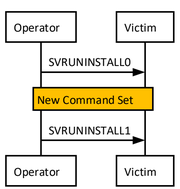


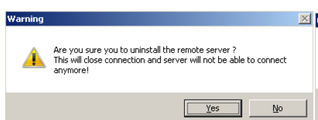
Server Actions -> Close Server

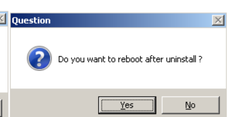




Server Actions -> Uninstall Server

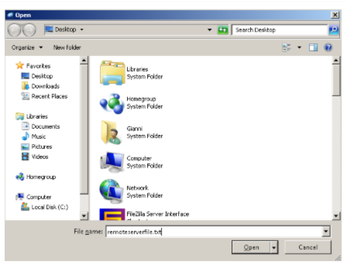




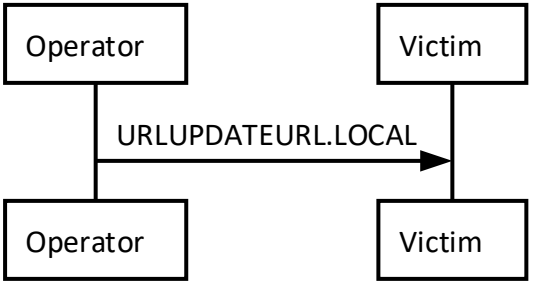


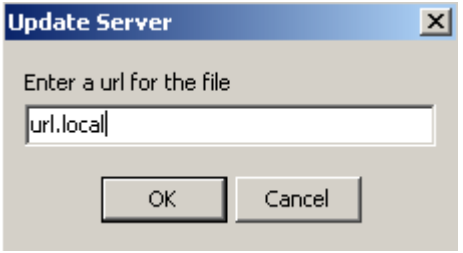
Server Actions -> Upload and Execute

Server Actions -> Remote Edit Server

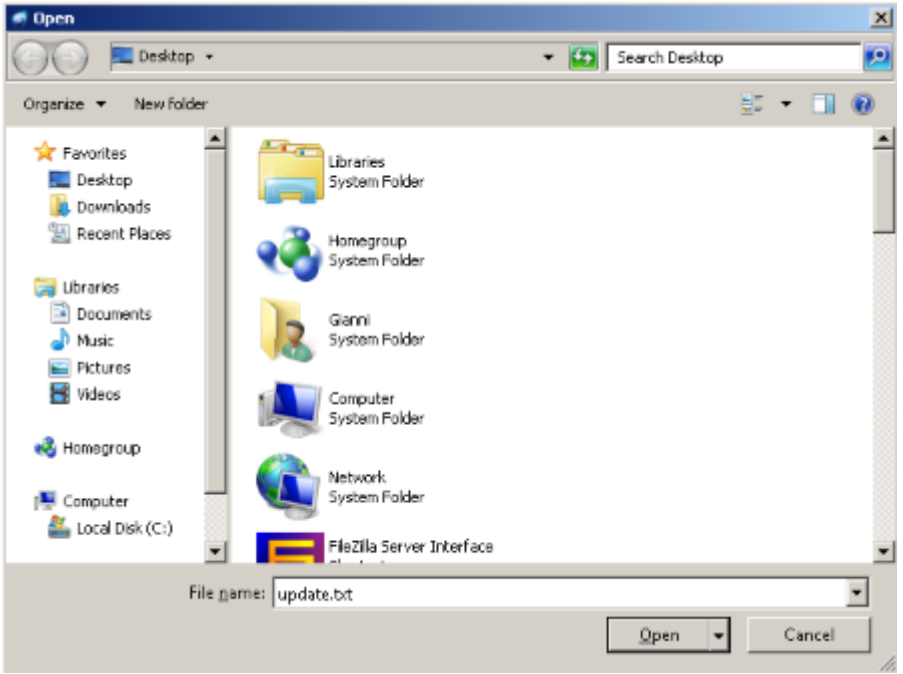


Update Server -> From URL



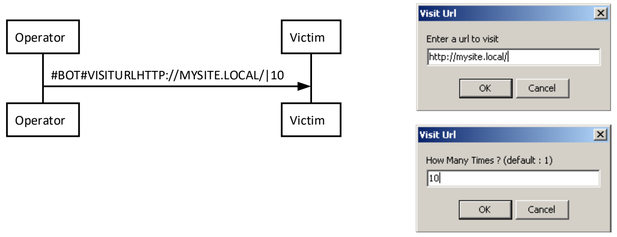


Update Server -> From File

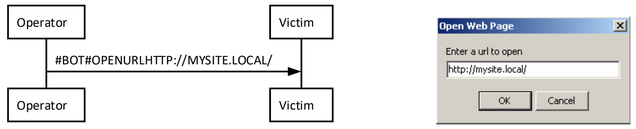


Extra Broadcast Commands

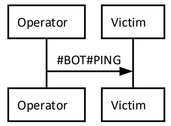
Extra Broadcast Commands -> Visit Website



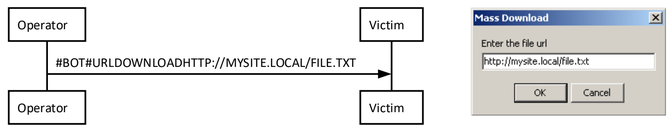
Extra Broadcast Commands -> Open Webpage



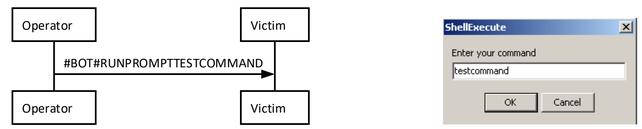
Extra Broadcast Commands -> Ping Server



Extra Broadcast Commands -> Mass Download



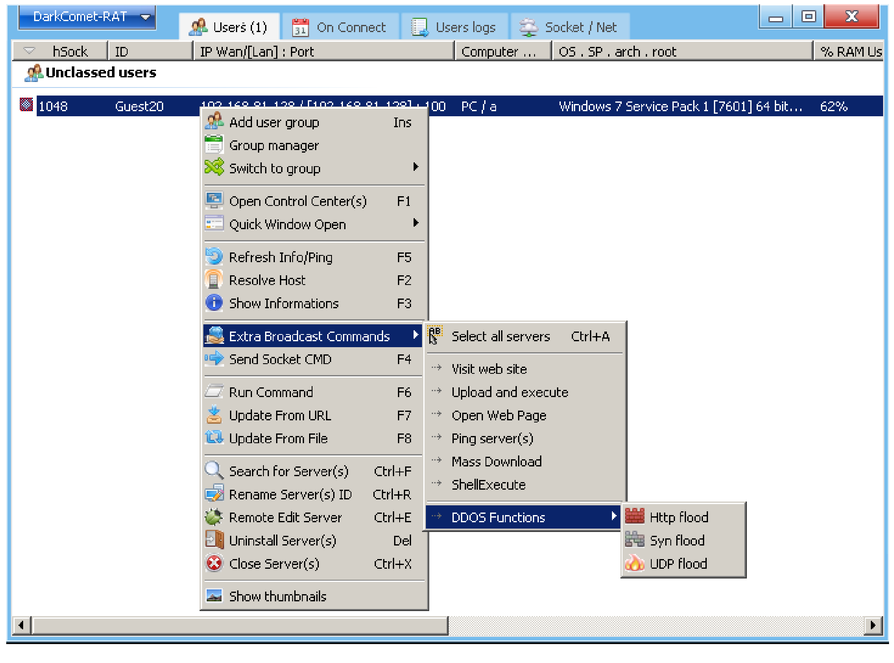
Extra Broadcast Commands -> Shell Execute



Extra Broadcast Commands -> DDOS Functions -> HTTP Flood

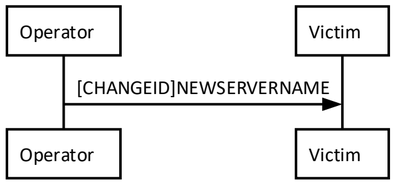
Extra Broadcast Commands -> DDOS Functions -> SYN Flood

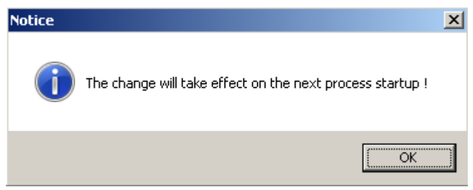
Extra Broadcast Commands -> DDOS Functions -> UDP Flood



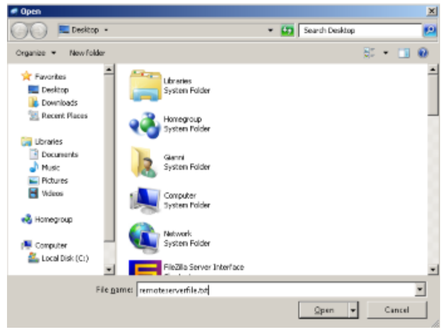
Other Commands

Change Server ID

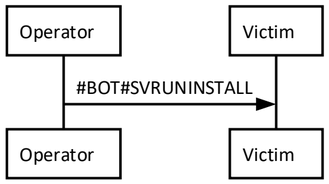


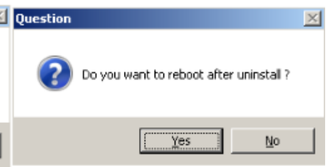


Edit Server



Uninstall Server





Close Server