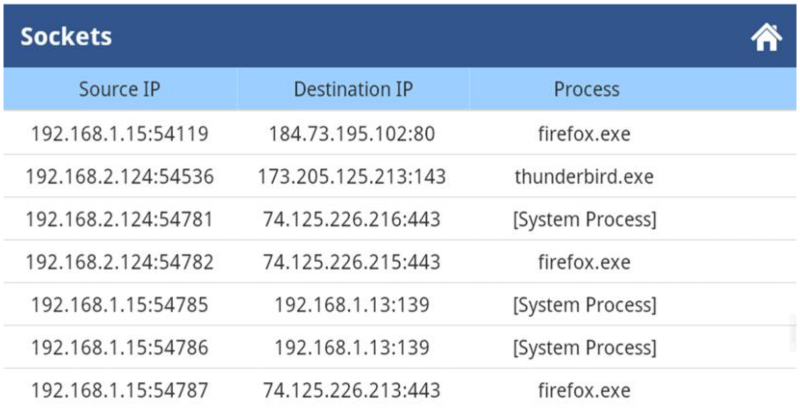
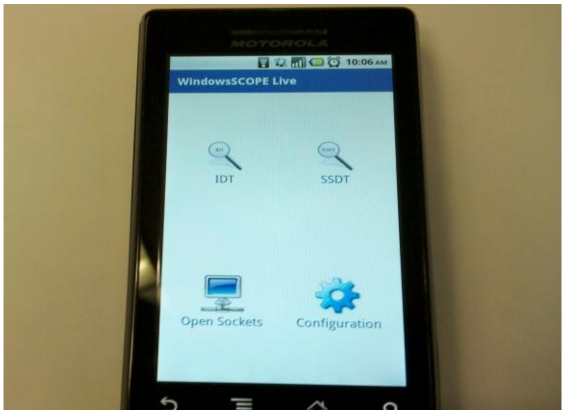
WindowsSCOPE Live
Real-Time Cyber Investigation and Memory Forensics

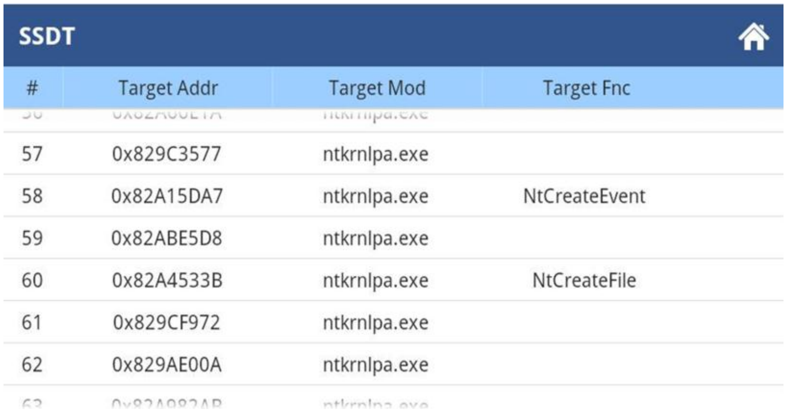
- **Live system analysis of Windows computers from your mobile device**
- **User-mode and kernel-mode capture techniques**
- **Same powerful memory capture capabilities as WindowsSCOPE**
- **Review kernel structures on demand to uncover system hooks**
- **Identify suspicious behavior**



Sockets

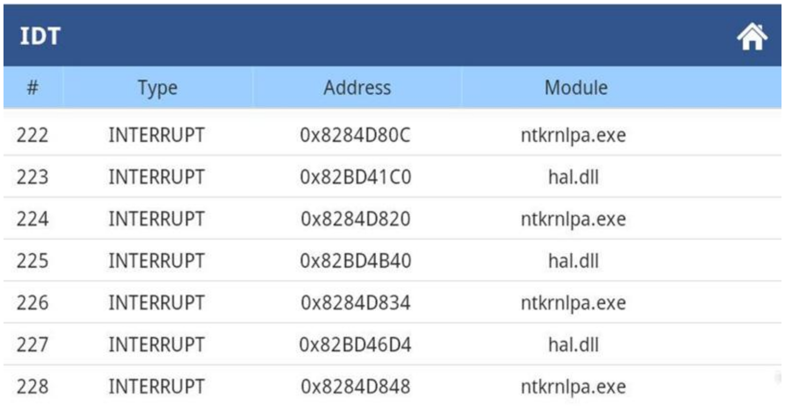
Source IP	Destination IP	Process
192.168.1.15:54119	184.73.195.102:80	firefox.exe
192.168.2.124:54536	173.205.125.213:143	thunderbird.exe
192.168.2.124:54781	74.125.226.216:443	[System Process]
192.168.2.124:54782	74.125.226.215:443	firefox.exe
192.168.1.15:54785	192.168.1.13:139	[System Process]
192.168.1.15:54786	192.168.1.13:139	[System Process]
192.168.1.15:54787	74.125.226.213:443	firefox.exe





SSDT

#	Target Addr	Target Mod	Target Fnc
56	0x82A00E1A	ntkrnlpa.exe	
57	0x829C3577	ntkrnlpa.exe	
58	0x82A15DA7	ntkrnlpa.exe	NtCreateEvent
59	0x82ABE5D8	ntkrnlpa.exe	
60	0x82A4533B	ntkrnlpa.exe	NtCreateFile
61	0x829CF972	ntkrnlpa.exe	
62	0x829AE00A	ntkrnlpa.exe	
63	0x82A982AB	ntkrnlpa.exe	



IDT

#	Type	Address	Module
222	INTERRUPT	0x8284D80C	ntkrnlpa.exe
223	INTERRUPT	0x82BD41C0	hal.dll
224	INTERRUPT	0x8284D820	ntkrnlpa.exe
225	INTERRUPT	0x82BD4B40	hal.dll
226	INTERRUPT	0x8284D834	ntkrnlpa.exe
227	INTERRUPT	0x82BD46D4	hal.dll
228	INTERRUPT	0x8284D848	ntkrnlpa.exe

Use Cases/Platforms Supported

- IT administrators managing many Windows workstations and servers
  - Create profiles to scan any number of Windows computers
  - Periodically check up on servers and other key infrastructure
  - No need to bring the system down while you investigate
- Quick cyber-analysis without having to be at the computer
  - Allow users to continue using their workstations while under investigation
- Identify indicators of compromise before doing in-depth analysis
- Supported platforms:
  - X86 and X64 Windows operating systems up to Windows 7
- All Android 2.1 or later mobile devices for the client
- Available now on the Android marketplace and at http://www.windowsscope.com

101 University Drive, Amherst, MA 01002, TEL: (413) 549-0599
FAX:(413)825-0217, sales@windowsscope.com, www.windowsscope.com