Windows SCOPE
Window into Windows

WindowsSCOPE 3.2 Cyber Forensics

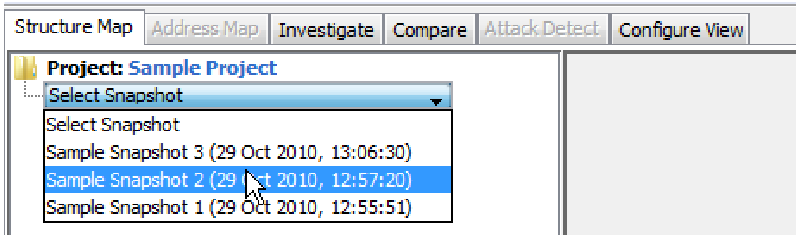
“Memory Forensics for Incidence Responders”

User Interface – Quick Guide

WindowsSCOPE reverse engineers raw memory dumps to analyze the internals of the Windows operating system and everything it runs. Use it to analyze the Windows kernel, virtual memory management, x86 memory management, device drivers and applications; access the kernel, disassemble and graph any code in the kernel or user space; verify applications' behavior at runtime in memory, analyze for malware/cyber-attacks, or perform memory forensics, and much more. The integrated data memory search tool enables automated extraction of usernames, passwords, visited websites, phone numbers, and customer regular-expression searches. The tool allows annotations and has an interactive graphing capability as well as several built-in analyses for cyber-attack finger printing.

Snapshot Repository

- Every memory snapshot captured is saved to the repository for future reference
- Compare feature - uses repository to enable comparing of any structure against the same structure in any previous snapshot
- …



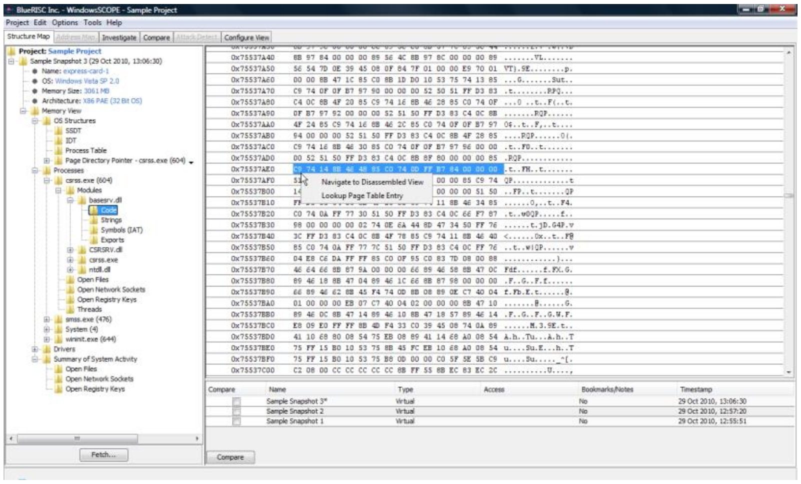
Project: Sample Project

Select Snapshot

Select Snapshot
Sample Snapshot 3 (29 Oct 2010, 13:06:30)
Sample Snapshot 2 (29 Oct 2010, 12:57:20)
Sample Snapshot 1 (29 Oct 2010, 12:55:51)

Structure Map

- Quick access to all structures captured in the memory snapshot including drivers, modules, processes, page tables, interrupt table, and system call table
- Quick navigation from raw code to the disassembled view by right clicking
- Compare any structure in the snapshot against the same structure in any previous snapshot
- Summary of system activity shows you all open files, network sockets, and registry keys
-



```
Project: Sample Project
Sample Snapshot 3 (29 Oct 2010, 13:06:30)
    Name: express-card-1
    OS: Windows Vista SP 2.0
    Memory Size: 3061 MB
    Architecture: X86 PAE (32 Bit OS)
    Memory View
        OS Structures
            SSDT
            IDT
            Process Table
            Page Directory Pointer - csrss.exe (604)
        Processes
            csrss.exe (604)
                Modules
                    basesrv.dll
                        Code
                        Strings
                        Symbols (IAT)
                        Exports
                    CSRSRV.dll
                    csrss.exe
                    ntdll.dll
                Open Files
                Open Network Sockets
                Open Registry Keys
                Threads
            smss.exe (476)
            System (4)
            wininit.exe (644)
        Drivers
        Summary of System Activity
            Open Files
            Open Network Sockets
            Open Registry Keys
```

```
0x75537A40   8B 97 84 00 00 00 89 56 4C 8B 97 8C 00 00 00 89   .......VL.......
0x75537A50   56 54 7D 0E 39 45 08 0F 84 7F 01 00 00 E9 70 01   VT}.9E........p.
0x75537A60   00 00 8B 47 1C 85 C0 8B 1D D0 10 53 75 74 13 85   ...G.......Sut..
0x75537A70   C9 74 0F 0F B7 97 90 00 00 00 52 50 51 FF D3 83   .t........RPQ...
0x75537A80   C4 0C 8B 4F 20 85 C9 74 16 8B 46 28 85 C0 74 0F   ...O ..t..F(..t.
0x75537A90   0F B7 97 92 00 00 00 52 51 50 FF D3 83 C4 0C 8B   .......RQP......
0x75537AA0   4F 24 85 C9 74 16 8B 46 2C 85 C0 74 0F 0F B7 97   O$..t..F,..t....
0x75537AB0   94 00 00 00 52 51 50 FF D3 83 C4 0C 8B 4F 28 85   ....RQP......O(.
0x75537AC0   C9 74 16 8B 46 30 85 C0 74 0F 0F B7 97 96 00 00   .t..F0..t.......
0x75537AD0   00 52 51 50 FF D3 83 C4 0C 8B 8F 80 00 00 00 85   .RQP............
0x75537AE0   C9 74 14 8B 46 48 85 C0 74 0D FF B7 84 00 00 00   .t..FH..t.......
0x75537AF0   51                            00 00 85 C9 74   QP.............t
0x75537B00   14                            00 00 00 51 50   ..FP..t.......QP
0x75537B10   FF                            11 8B 46 34 85   ......O,..t..F4.
0x75537B20   C0 74 0A FF 77 30 51 50 FF D3 83 C4 0C 66 F7 87   .t..w0QP.....f..
0x75537B30   98 00 00 00 00 02 74 0E 6A 44 8D 47 34 50 FF 76   ......t.jD.G4P.v
0x75537B40   3C FF D3 83 C4 0C 8B 4F 78 85 C9 74 11 8B 46 40   <......Ox..t..F@
0x75537B50   85 C0 74 0A FF 77 7C 51 50 FF D3 83 C4 0C FF 76   ..t..w|QP......v
0x75537B60   04 E8 C6 DA FF FF 85 C0 0F 95 C0 83 7D 08 00 88   ............}...
0x75537B70   46 64 66 8B 87 9A 00 00 00 66 89 46 58 8B 47 0C   Fdf......f.FX.G.
0x75537B80   89 46 18 8B 47 04 89 46 1C 66 8B 87 98 00 00 00   .F..G..F.f......
0x75537B90   66 89 46 62 8B 45 F4 74 0D 8B 08 89 0E C7 40 04   f.Fb.E.t......@.
0x75537BA0   01 00 00 00 EB 07 C7 40 04 02 00 00 00 8B 47 10   .......@......G.
0x75537BB0   89 46 0C 8B 47 14 89 46 10 8B 47 18 57 89 46 14   .F..G..F..G.W.F.
0x75537BC0   E8 09 E0 FF FF 8B 4D F4 33 C0 39 45 08 74 0A 89   ......M.3.9E.t..
0x75537BD0   41 10 68 80 08 54 75 EB 08 89 41 14 68 A0 08 54   A.h..Tu...A.h..T
0x75537BE0   75 FF 15 B0 10 53 75 8B 45 FC EB 10 68 A0 08 54   u....Su.E...h..T
0x75537BF0   75 FF 15 B0 10 53 75 B8 0D 00 00 C0 5F 5E 5B C9   u....Su....._^[.
0x75537C00   C2 08 00 CC CC CC CC CC 8B FF 55 8B EC 83 EC 2C   ..........U....,
```

Compare	Name	Type	Access	Bookmarks/Notes	Timestamp
☐	Sample Snapshot 3*	Virtual		No	29 Oct 2010, 13:06:30
☐	Sample Snapshot 2	Virtual		No	29 Oct 2010, 12:57:20
☐	Sample Snapshot 1	Virtual		No	29 Oct 2010, 12:55:51

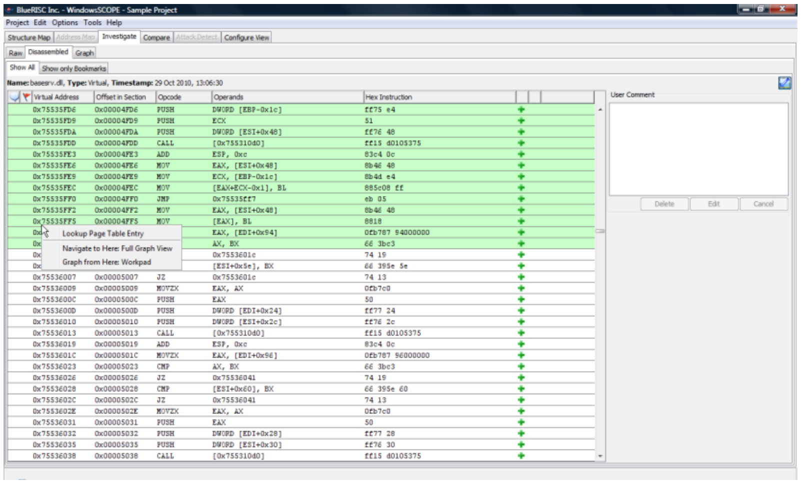
Data Search

- Find artifacts hidden in live memory – Passwords, encryption keys, etc.
- Uncover recent activity – URLs, phone numbers, email addresses, etc.
- …

Disassembled View

- Complete view of all instructions including opcodes, operands, and hex encodings
- Highlighting to show which instructions were in physical memory at the time of the fetch
- Quickly find memory attributes and physical mappings by right clicking to lookup page table entries for any instruction
- Quickly visualize program behavior by right clicking to navigate either to the full graph or workpad graph views

…

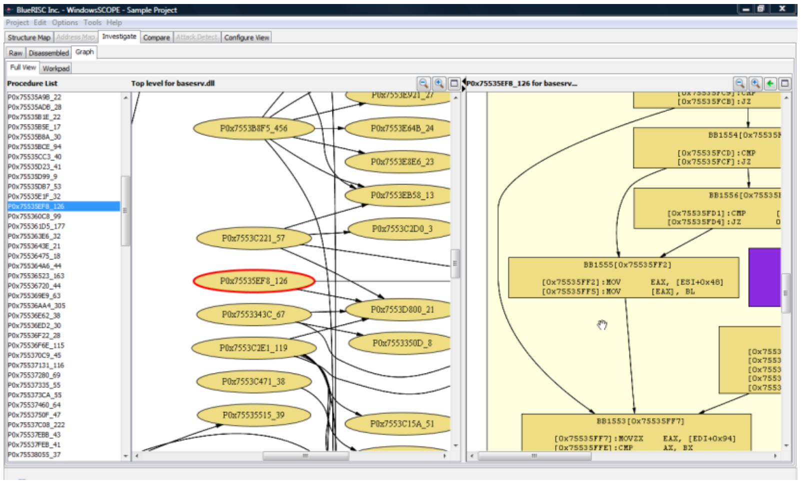


Name: basesrv.dll, **Type:** Virtual, **Timestamp:** 29 Oct 2010, 13:06:30

Virtual Address	Offset in Section	Opcode	Operands	Hex Instruction
0x75535FD6	0x00004FD6	PUSH	DWORD [EBP-0x1c]	ff75 e4
0x75535FD9	0x00004FD9	PUSH	ECX	51
0x75535FDA	0x00004FDA	PUSH	DWORD [ESI+0x48]	ff76 48
0x75535FDD	0x00004FDD	CALL	[0x755310d0]	ff15 d0105375
0x75535FE3	0x00004FE3	ADD	ESP, 0xc	83c4 0c
0x75535FE6	0x00004FE6	MOV	EAX, [ESI+0x48]	8b46 48
0x75535FE9	0x00004FE9	MOV	ECX, [EBP-0x1c]	8b4d e4
0x75535FEC	0x00004FEC	MOV	[EAX+ECX-0x1], BL	885c08 ff
0x75535FF0	0x00004FF0	JMP	0x75535ff7	eb 05
0x75535FF2	0x00004FF2	MOV	EAX, [ESI+0x48]	8b46 48
0x75535FF5	0x00004FF5	MOV	[EAX], BL	8818
0x			EAX, [EDI+0x94]	0fb787 94000000
0x			AX, BX	66 3bc3
0x			0x7553601c	74 19
0x			[ESI+0x5e], BX	66 395e 5e
0x75536007	0x00005007	JZ	0x7553601c	74 13
0x75536009	0x00005009	MOVZX	EAX, AX	0fb7c0
0x7553600C	0x0000500C	PUSH	EAX	50
0x7553600D	0x0000500D	PUSH	DWORD [EDI+0x24]	ff77 24
0x75536010	0x00005010	PUSH	DWORD [ESI+0x2c]	ff76 2c
0x75536013	0x00005013	CALL	[0x755310d0]	ff15 d0105375
0x75536019	0x00005019	ADD	ESP, 0xc	83c4 0c
0x7553601C	0x0000501C	MOVZX	EAX, [EDI+0x96]	0fb787 96000000
0x75536023	0x00005023	CMP	AX, BX	66 3bc3
0x75536026	0x00005026	JZ	0x75536041	74 19
0x75536028	0x00005028	CMP	[ESI+0x60], BX	66 395e 60
0x7553602C	0x0000502C	JZ	0x75536041	74 13
0x7553602E	0x0000502E	MOVZX	EAX, AX	0fb7c0
0x75536031	0x00005031	PUSH	EAX	50
0x75536032	0x00005032	PUSH	DWORD [EDI+0x28]	ff77 28
0x75536035	0x00005035	PUSH	DWORD [ESI+0x30]	ff76 30
0x75536038	0x00005038	CALL	[0x755310d0]	ff15 d0105375

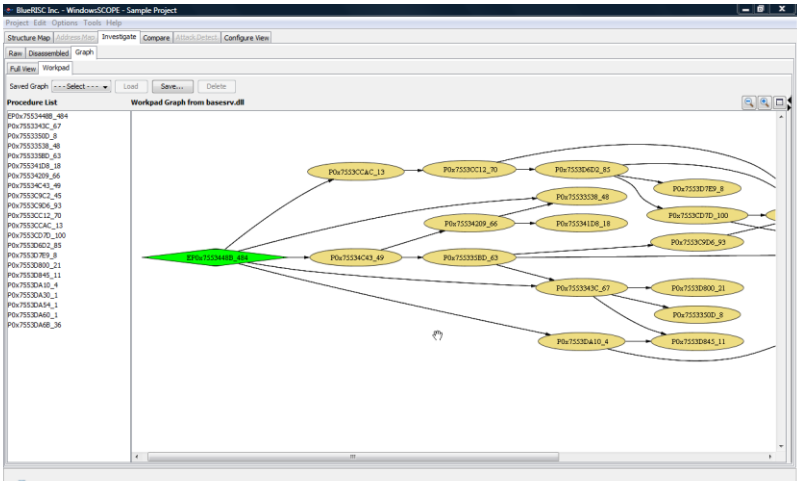
Graph View

- Complete control-flow graph generation covering all executable sections of executables, DLLs, and drivers
- Locate procedures either by address using a sorted list or by selecting them from the binary's call graph
- Procedures listed in the binary's export table are shown by name
- Interactive graph navigation using mouse controls and clickable nodes
- Split view for viewing call graph and the control flow of a selected procedure simultaneously, and just one click to maximize either view
- …



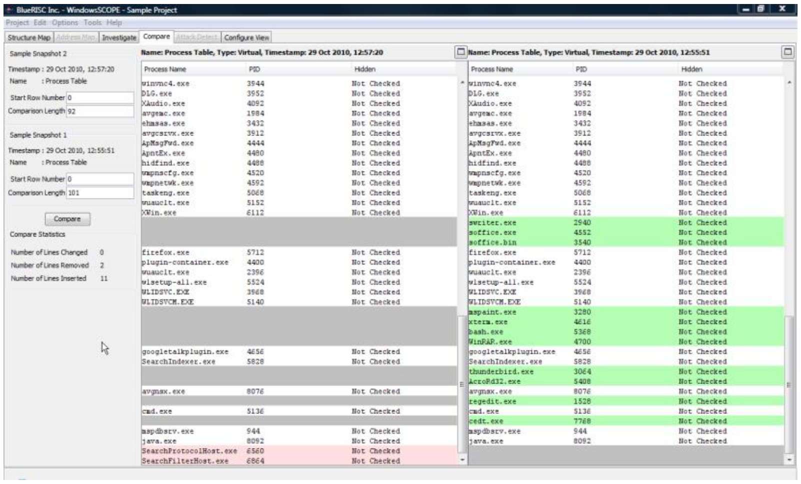
Workpad View

- Save time when graphing binaries by only graphing parts of interest
- Start a workpad graph from any instruction in a binary from the disassembled view with a right-click
- Workpad graphs are fast and easy – each new graph can be generated in seconds
- Workpad graphs are smaller and less complicated than full graphs, putting the focus on the parts of an application that matter
- Any graph generated in the workpad can be saved for later use



Compare View

- Compare any structure in the snapshot against the same structure in any previous snapshot
- Each comparison can be uniquely configured by specifying which row to start the comparison on and the number of rows to compare
- Side by side view with highlighting to indicate rows that have been added, removed, or modified
- Detailed comparison results indicating the number of rows that have been changed, inserted, and removed


BlueRISC Inc. - WindowsSCOPE - Sample Project
Project Edit Options Tools Help
Structure Map
Address Map
Investigate
Compare
Attack Detect
Configure View
Compare

Sample Snapshot 2

Timestamp : 29 Oct 2010, 12:57:20
Name : Process Table
Start Row Number 0
Comparison Length 92

Sample Snapshot 1

Timestamp : 29 Oct 2010, 12:55:51
Name : Process Table
Start Row Number 0
Comparison Length 101

Compare Statistics

Number of Lines Changed	0
Number of Lines Removed	2
Number of Lines Inserted	11

Name: Process Table, Type: Virtual, Timestamp: 29 Oct 2010, 12:57:20

Process Name	PID	Hidden
winvnc4.exe	3944	Not Checked
DLG.exe	3952	Not Checked
XAudio.exe	4092	Not Checked
avgemc.exe	1984	Not Checked
ehmsas.exe	3432	Not Checked
avgcsrvx.exe	3912	Not Checked
ApMsgFwd.exe	4444	Not Checked
ApntEx.exe	4480	Not Checked
hidfind.exe	4488	Not Checked
wmpnscfg.exe	4520	Not Checked
wmpnetwk.exe	4592	Not Checked
taskeng.exe	5068	Not Checked
wuauclt.exe	5152	Not Checked
XWin.exe	6112	Not Checked
firefox.exe	5712	Not Checked
plugin-container.exe	4400	Not Checked
wuauclt.exe	2396	Not Checked
wlsetup-all.exe	5524	Not Checked
WLIDSVC.EXE	3968	Not Checked
WLIDSVCM.EXE	5140	Not Checked
googletalkplugin.exe	4656	Not Checked
SearchIndexer.exe	5828	Not Checked
avgnsx.exe	8076	Not Checked
cmd.exe	5136	Not Checked
mspdbsrv.exe	944	Not Checked
java.exe	8092	Not Checked
SearchProtocolHost.exe	6560	Not Checked
SearchFilterHost.exe	6864	Not Checked

Name: Process Table, Type: Virtual, Timestamp: 29 Oct 2010, 12:55:51

Process Name	PID	Hidden
winvnc4.exe	3944	Not Checked
DLG.exe	3952	Not Checked
XAudio.exe	4092	Not Checked
avgemc.exe	1984	Not Checked
ehmsas.exe	3432	Not Checked
avgcsrvx.exe	3912	Not Checked
ApMsgFwd.exe	4444	Not Checked
ApntEx.exe	4480	Not Checked
hidfind.exe	4488	Not Checked
wmpnscfg.exe	4520	Not Checked
wmpnetwk.exe	4592	Not Checked
taskeng.exe	5068	Not Checked
wuauclt.exe	5152	Not Checked
XWin.exe	6112	Not Checked
swriter.exe	2940	Not Checked
soffice.exe	4552	Not Checked
soffice.bin	3540	Not Checked
firefox.exe	5712	Not Checked
plugin-container.exe	4400	Not Checked
wuauclt.exe	2396	Not Checked
wlsetup-all.exe	5524	Not Checked
WLIDSVC.EXE	3968	Not Checked
WLIDSVCM.EXE	5140	Not Checked
mspaint.exe	3280	Not Checked
xterm.exe	4616	Not Checked
bash.exe	5368	Not Checked
WinRAR.exe	4700	Not Checked
googletalkplugin.exe	4656	Not Checked
SearchIndexer.exe	5828	Not Checked
thunderbird.exe	3064	Not Checked
AcroRd32.exe	5408	Not Checked
avgnsx.exe	8076	Not Checked
regedit.exe	1528	Not Checked
cmd.exe	5136	Not Checked
cedt.exe	7768	Not Checked
mspdbsrv.exe	944	Not Checked
java.exe	8092	Not Checked

400 Amity St, Amherst, MA 01002,
TEL: (413) 359-0599
FAX: (413) 825-0217, sales@windowsscope.com