Introduction to Digital Forensic Tools

Mark Pollitt

Associate Professor

DF Tools Philosophy

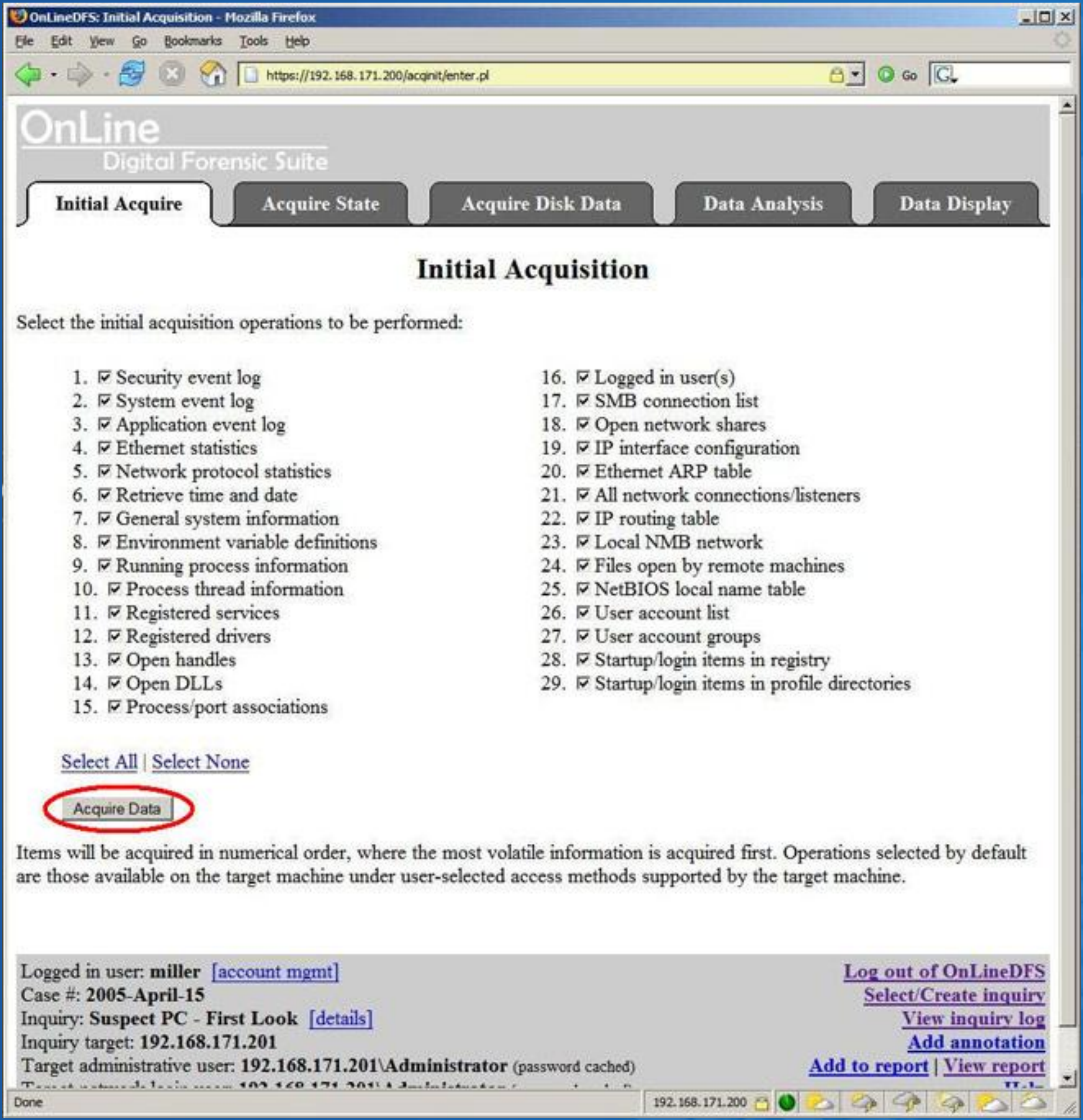
- DF Software are tools NOT solutions
- Picking the right tool for the job is important
- Competence in using the tool is more important than the number of tools in your “toolbox.”
- Balancing act in ease of use, utility, and efficiency.

Tool Functions

- Data acquisition
- Validation/discrimination (Nelson, et al.)
- Data extraction
- Reconstruction
- Analysis
- Reporting (Nelson, et al.) NOT!

Tool Classification

- Operating system tools
  - DD, grep, fstat, md5sum, etc.
- Command line tools
  - Hama, Maresware, Sleuthkit
- Hex editors
  - WinHex, Diskedit
- Integrated GUI
  - Encase, FTK, Prodiscover
- Network based tools
  - Enterprise Encase/FTK, OnLineDFS
- Mobile Devices
  - Paraben, XRY, Encase, FTK


OnLineDFS: Initial Acquisition - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://192.168.171.200/acqinit/enter.pl
Go
OnLine
Digital Forensic Suite
Initial Acquire
Acquire State
Acquire Disk Data
Data Analysis
Data Display

Initial Acquisition

Select the initial acquisition operations to be performed:

1. ☑ Security event log
2. ☑ System event log
3. ☑ Application event log
4. ☑ Ethernet statistics
5. ☑ Network protocol statistics
6. ☑ Retrieve time and date
7. ☑ General system information
8. ☑ Environment variable definitions
9. ☑ Running process information
10. ☑ Process thread information
11. ☑ Registered services
12. ☑ Registered drivers
13. ☑ Open handles
14. ☑ Open DLLs
15. ☑ Process/port associations
16. ☑ Logged in user(s)
17. ☑ SMB connection list
18. ☑ Open network shares
19. ☑ IP interface configuration
20. ☑ Ethernet ARP table
21. ☑ All network connections/listeners
22. ☑ IP routing table
23. ☑ Local NMB network
24. ☑ Files open by remote machines
25. ☑ NetBIOS local name table
26. ☑ User account list
27. ☑ User account groups
28. ☑ Startup/login items in registry
29. ☑ Startup/login items in profile directories

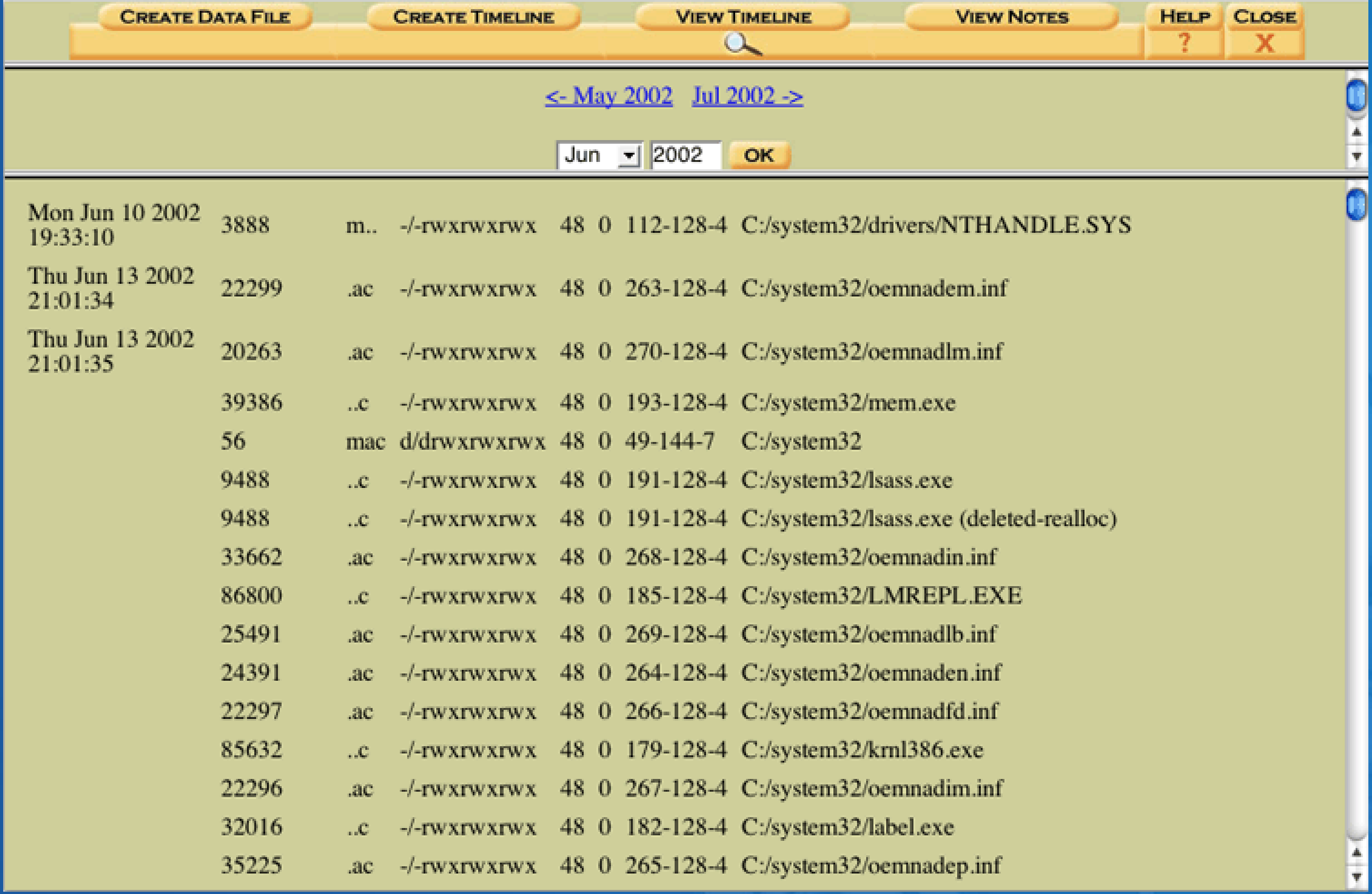
Select All | Select None

Items will be acquired in numerical order, where the most volatile information is acquired first. Operations selected by default are those available on the target machine under user-selected access methods supported by the target machine.

Logged in user: **miller** [account mgmt]
Case #: **2005-April-15**
Inquiry: **Suspect PC - First Look** [details]
Inquiry target: **192.168.171.201**
Target administrative user: **192.168.171.201\Administrator** (password cached)

http://www.cyberstc.com/tour_04.asp

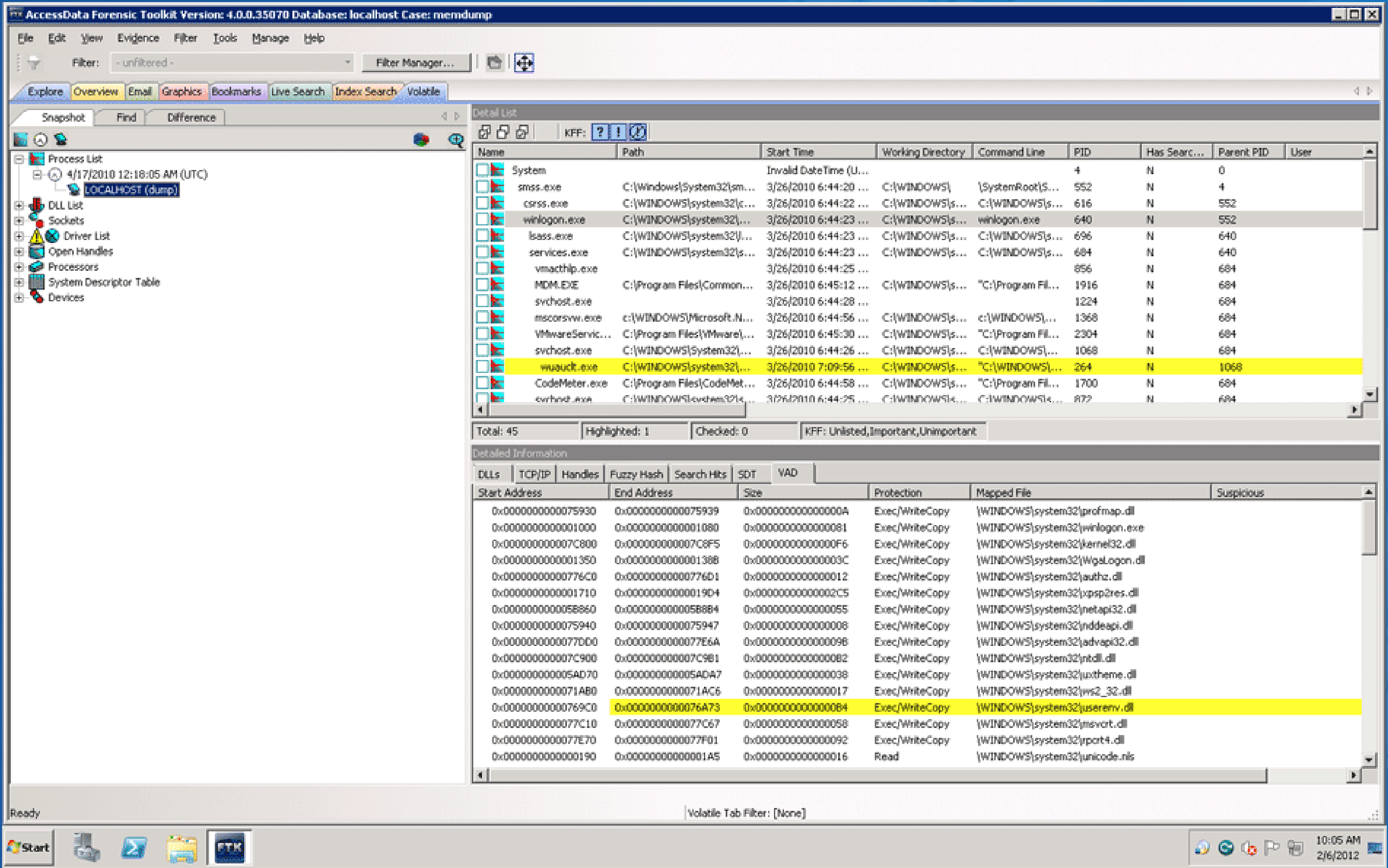
Autopsy Browser



```
Mon Jun 10 2002
19:33:10         3888    m..  -/-rwxrwxrwx  48 0 112-128-4 C:/system32/drivers/NTHANDLE.SYS
Thu Jun 13 2002
21:01:34         22299   .ac  -/-rwxrwxrwx  48 0 263-128-4 C:/system32/oemnadem.inf
Thu Jun 13 2002
21:01:35         20263   .ac  -/-rwxrwxrwx  48 0 270-128-4 C:/system32/oemnadlm.inf
                 39386   ..c  -/-rwxrwxrwx  48 0 193-128-4 C:/system32/mem.exe
                 56      mac  d/drwxrwxrwx  48 0 49-144-7  C:/system32
                 9488    ..c  -/-rwxrwxrwx  48 0 191-128-4 C:/system32/lsass.exe
                 9488    ..c  -/-rwxrwxrwx  48 0 191-128-4 C:/system32/lsass.exe (deleted-realloc)
                 33662   .ac  -/-rwxrwxrwx  48 0 268-128-4 C:/system32/oemnadin.inf
                 86800   ..c  -/-rwxrwxrwx  48 0 185-128-4 C:/system32/LMREPL.EXE
                 25491   .ac  -/-rwxrwxrwx  48 0 269-128-4 C:/system32/oemnadlb.inf
                 24391   .ac  -/-rwxrwxrwx  48 0 264-128-4 C:/system32/oemnaden.inf
                 22297   .ac  -/-rwxrwxrwx  48 0 266-128-4 C:/system32/oemnadfd.inf
                 85632   ..c  -/-rwxrwxrwx  48 0 179-128-4 C:/system32/krnl386.exe
                 22296   .ac  -/-rwxrwxrwx  48 0 267-128-4 C:/system32/oemnadim.inf
                 32016   ..c  -/-rwxrwxrwx  48 0 182-128-4 C:/system32/label.exe
                 35225   .ac  -/-rwxrwxrwx  48 0 265-128-4 C:/system32/oemnadep.inf
```

http://www.sleuthkit.org/autopsy/images/timeline1.gif

GUI - FTK



AccessData Forensic Toolkit Version: 4.0.0.35070 Database: localhost Case: memdump

Name	Path	Start Time	Working Directory	Command Line	PID	Has Searc...	Parent PID	User
☐ System		Invalid DateTime (U...			4	N	0	
☐ smss.exe	C:\Windows\System32\sm...	3/26/2010 6:44:20 ...	C:\WINDOWS\	\SystemRoot\S...	552	N	4	
☐ csrss.exe	C:\WINDOWS\system32\c...	3/26/2010 6:44:22 ...	C:\WINDOWS\s...	C:\WINDOWS\s...	616	N	552	
☐ winlogon.exe	C:\WINDOWS\system32\...	3/26/2010 6:44:23 ...	C:\WINDOWS\s...	winlogon.exe	640	N	552	
☐ lsass.exe	C:\WINDOWS\system32\l...	3/26/2010 6:44:23 ...	C:\WINDOWS\s...	C:\WINDOWS\s...	696	N	640	
☐ services.exe	C:\WINDOWS\system32\s...	3/26/2010 6:44:23 ...	C:\WINDOWS\s...	C:\WINDOWS\s...	684	N	640	
☐ vmacthlp.exe		3/26/2010 6:44:25 ...			856	N	684	
☐ MDM.EXE	C:\Program Files\Common...	3/26/2010 6:45:12 ...	C:\WINDOWS\s...	"C:\Program Fil...	1916	N	684	
☐ svchost.exe		3/26/2010 6:44:28 ...			1224	N	684	
☐ mscorsvw.exe	c:\WINDOWS\Microsoft.N...	3/26/2010 6:44:56 ...	C:\WINDOWS\s...	c:\WINDOWS\...	1368	N	684	
☐ VMwareServic...	C:\Program Files\VMware\...	3/26/2010 6:45:30 ...	C:\WINDOWS\s...	"C:\Program Fil...	2304	N	684	
☐ svchost.exe	C:\WINDOWS\System32\...	3/26/2010 6:44:26 ...	C:\WINDOWS\s...	C:\WINDOWS\...	1068	N	684	
☐ wuauclt.exe	C:\WINDOWS\system32\...	3/26/2010 7:09:56 ...	C:\WINDOWS\s...	"C:\WINDOWS\...	264	N	1068	
☐ CodeMeter.exe	C:\Program Files\CodeMet...	3/26/2010 6:44:58 ...	C:\WINDOWS\s...	"C:\Program Fil...	1700	N	684	
☐ svchost.exe	C:\WINDOWS\system32\s...	3/26/2010 6:44:25 ...	C:\WINDOWS\s...	C:\WINDOWS\s...	872	N	684	

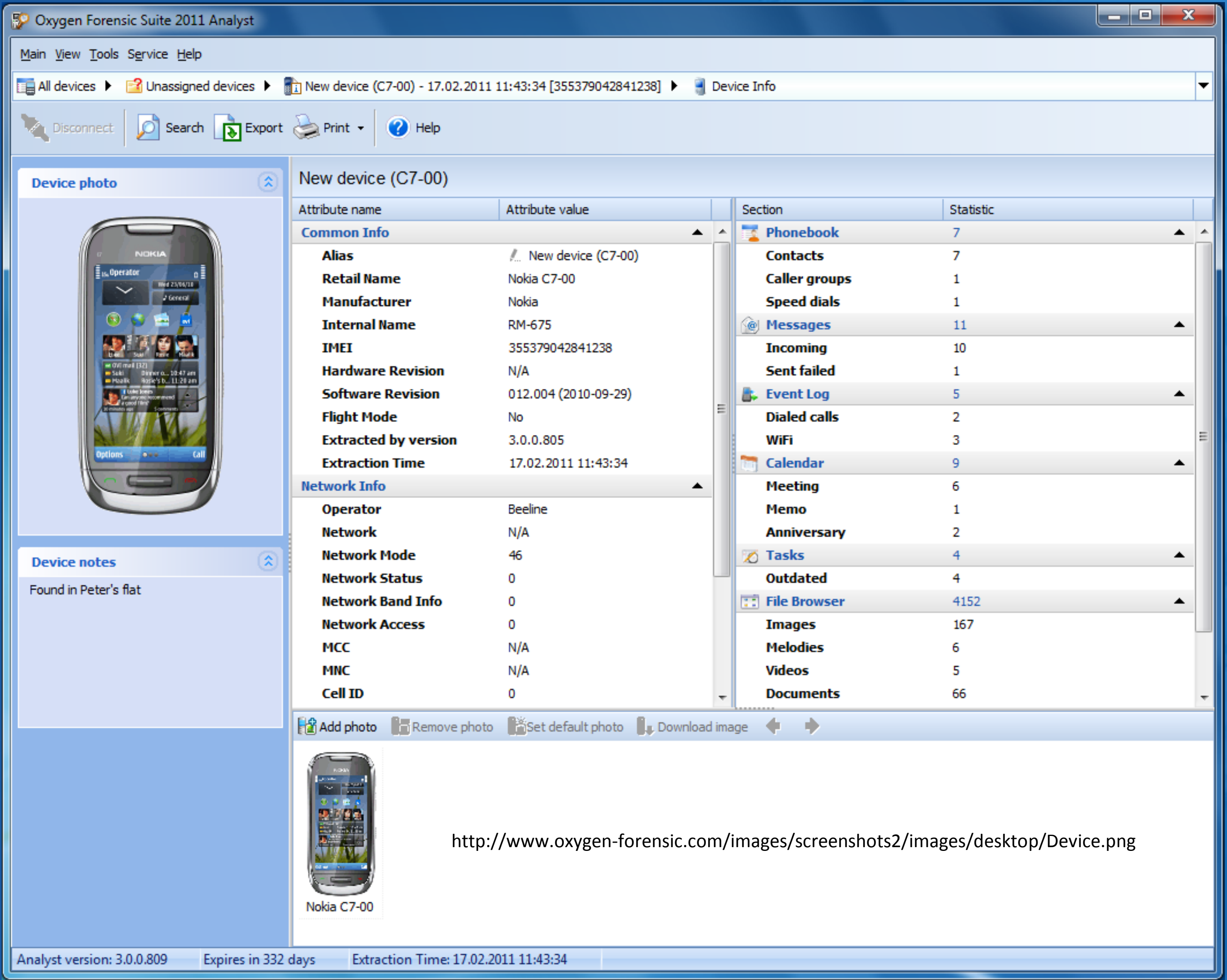
Total: 45 | Highlighted: 1 | Checked: 0 | KFF: Unlisted,Important,Unimportant

Start Address	End Address	Size	Protection	Mapped File	Suspicious
0x0000000000075930	0x0000000000075939	0x000000000000000A	Exec/WriteCopy	\WINDOWS\system32\profmap.dll	
0x0000000000001000	0x0000000000001080	0x0000000000000081	Exec/WriteCopy	\WINDOWS\system32\winlogon.exe	
0x000000000007C800	0x000000000007C8F5	0x00000000000000F6	Exec/WriteCopy	\WINDOWS\system32\kernel32.dll	
0x0000000000001350	0x000000000000138B	0x000000000000003C	Exec/WriteCopy	\WINDOWS\system32\WgaLogon.dll	
0x00000000000776C0	0x00000000000776D1	0x0000000000000012	Exec/WriteCopy	\WINDOWS\system32\authz.dll	
0x0000000000001710	0x00000000000019D4	0x00000000000002C5	Exec/WriteCopy	\WINDOWS\system32\xpsp2res.dll	
0x0000000000058860	0x00000000000588B4	0x0000000000000055	Exec/WriteCopy	\WINDOWS\system32\netapi32.dll	
0x0000000000075940	0x0000000000075947	0x0000000000000008	Exec/WriteCopy	\WINDOWS\system32\nddeapi.dll	
0x0000000000077DD0	0x0000000000077E6A	0x000000000000009B	Exec/WriteCopy	\WINDOWS\system32\advapi32.dll	
0x000000000007C900	0x000000000007C9B1	0x00000000000000B2	Exec/WriteCopy	\WINDOWS\system32\ntdll.dll	
0x000000000005AD70	0x000000000005ADA7	0x0000000000000038	Exec/WriteCopy	\WINDOWS\system32\uxtheme.dll	
0x0000000000071AB0	0x0000000000071AC6	0x0000000000000017	Exec/WriteCopy	\WINDOWS\system32\ws2_32.dll	
0x00000000000769C0	0x0000000000076A73	0x00000000000000B4	Exec/WriteCopy	\WINDOWS\system32\userenv.dll	
0x0000000000077C10	0x0000000000077C67	0x0000000000000058	Exec/WriteCopy	\WINDOWS\system32\msvcrt.dll	
0x0000000000077E70	0x0000000000077F01	0x0000000000000092	Exec/WriteCopy	\WINDOWS\system32\rpcrt4.dll	
0x0000000000000190	0x00000000000001A5	0x0000000000000016	Read	\WINDOWS\system32\unicode.nls	

Ready

Volatile Tab Filter: [None]

Mobile Device - Oxygen


Oxygen Forensic Suite 2011 Analyst
Main View Tools Service Help
All devices ▸ Unassigned devices ▸ New device (C7-00) - 17.02.2011 11:43:34 [355379042841238] ▸ Device Info
Disconnect
Search
Export
Print
Help
Device photo
Device notes
Add photo
Remove photo
Set default photo
Download image
Nokia C7-00

Found in Peter's flat

New device (C7-00)

Attribute name	Attribute value
Common Info	
Alias	New device (C7-00)
Retail Name	Nokia C7-00
Manufacturer	Nokia
Internal Name	RM-675
IMEI	355379042841238
Hardware Revision	N/A
Software Revision	012.004 (2010-09-29)
Flight Mode	No
Extracted by version	3.0.0.805
Extraction Time	17.02.2011 11:43:34
Network Info	
Operator	Beeline
Network	N/A
Network Mode	46
Network Status	0
Network Band Info	0
Network Access	0
MCC	N/A
MNC	N/A
Cell ID	0

Section	Statistic
Phonebook	7
Contacts	7
Caller groups	1
Speed dials	1
Messages	11
Incoming	10
Sent failed	1
Event Log	5
Dialed calls	2
WiFi	3
Calendar	9
Meeting	6
Memo	1
Anniversary	2
Tasks	4
Outdated	4
File Browser	4152
Images	167
Melodies	6
Videos	5
Documents	66

Analyst version: 3.0.0.809 | Expires in 332 days | Extraction Time: 17.02.2011 11:43:34

http://www.oxygen-forensic.com/images/screenshots2/images/desktop/Device.png

Hardware

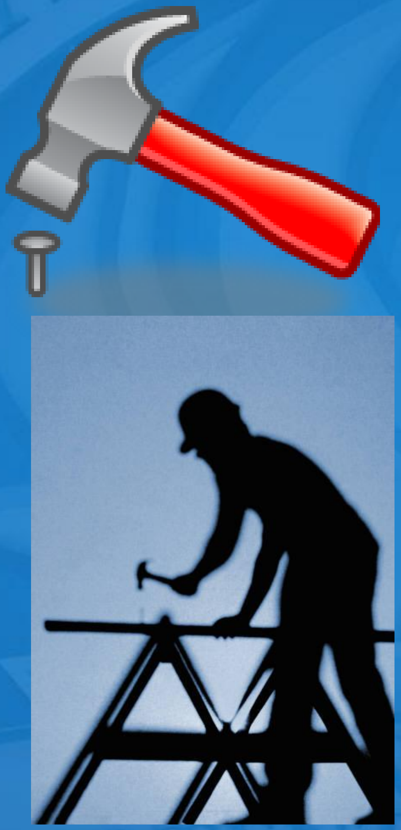
- Workstations
  - Desktop
  - Virtual
  - Cloud
- Portable Acquisitions
- Write Blockers

Digital Intelligence, Inc.
F.R.E.D.
Forensic Recovery of Evidence Device
intel

Remember…

It’s not the tool,

It’s the Carpenter!



Thanks for listening!