

Recent developments in volatile memory forensics

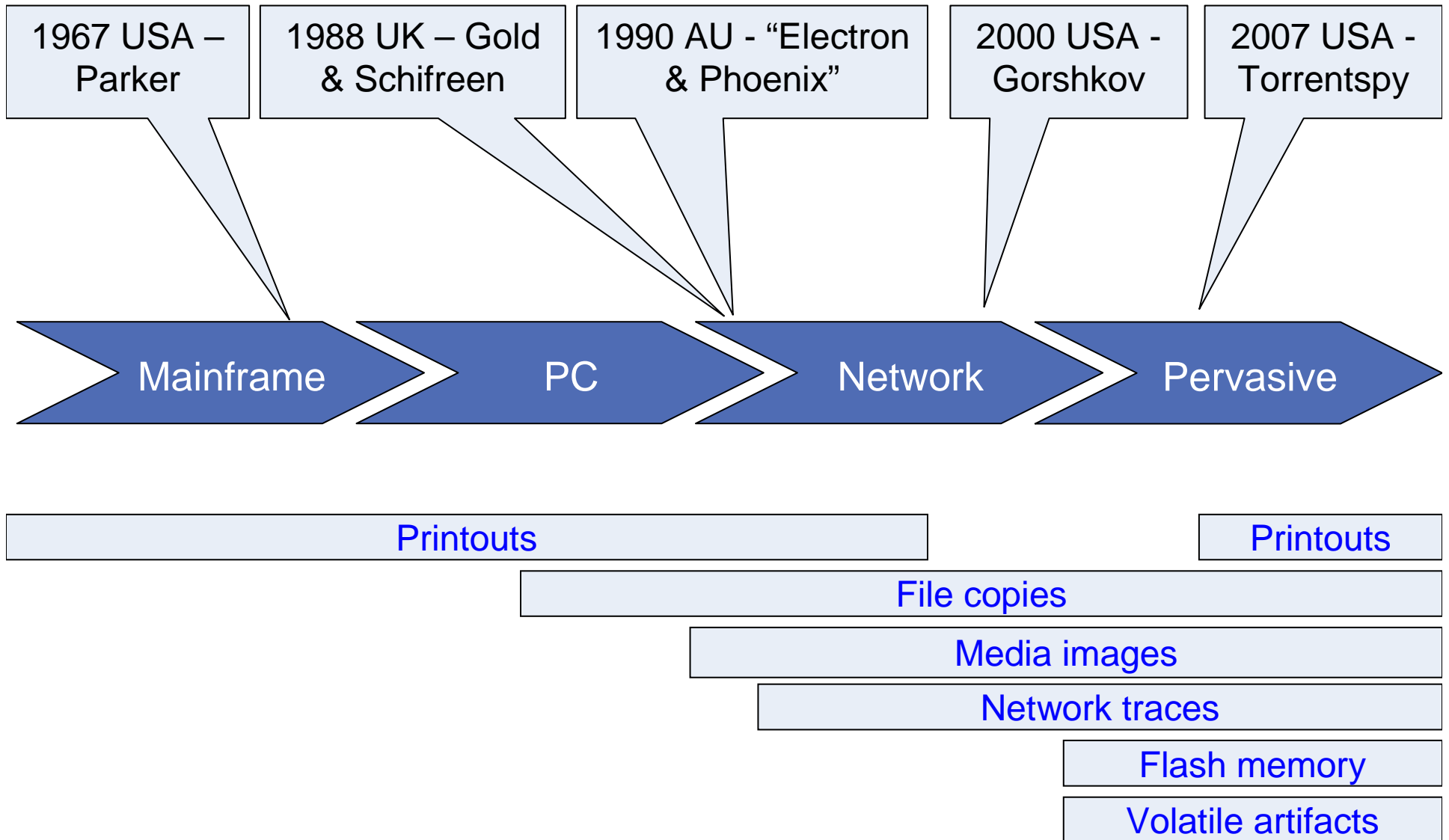
Bradley Schatz B.Sc.
Director, [Evimetry](#)
bradley.schatz@evimetry.com.au

- **Bradley Schatz**
 - Ph.D. (Computer Forensics) recently completed
 - Now practice computer forensics @ evimetry
 - Ongoing research in volatile memory forensics

- History of computer forensics & digital evidence
- Forensic practise
- Volatile memory forensics

Computer forensics

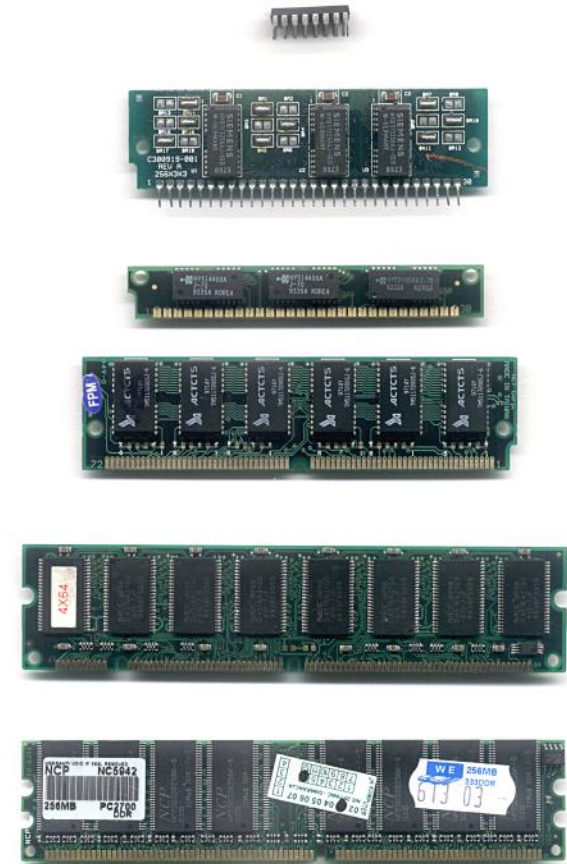
Evolution of computer evidence

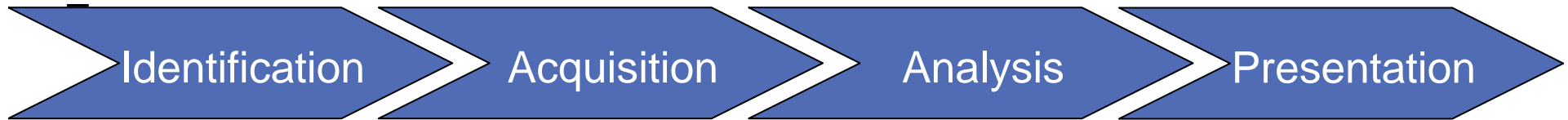




- Crime or misuse observed
- Identify potential evidence
- Plug pulled
- Hard drive imaged
- Detailed analysis of image
- Reporting of findings

- Running processes
- Network connections
- Open network ports
- Open files
- Loaded modules (DLL's)
- Dynamic Configuration
- PC Time
- ...





- Crime or misuse observed
- Identify potential evidence
- ***Live response performed***
- Plug pulled
- Hard drive imaged
- Detailed analysis of image
- Reporting of findings

- Tools
 - Sysinternals, foundstone
 - WFT
 - Helix
 - Wetstone, Mandiant, Guidance...
- Limitations:
 - System impact
 - Mixes analysis results with data acquisition
 - Not reproducible
 - OS trust

Application

1994 SunOS Application Rootkit
(CA-1994-01)

Kernel

1997 Linux Bugtraq (heroin.c)
1999 Linux Knark mass exploitation

Virtualisation

2005 Subvirt (VMware + VirtualPC)
2006 Bluepill (AMD + VT)

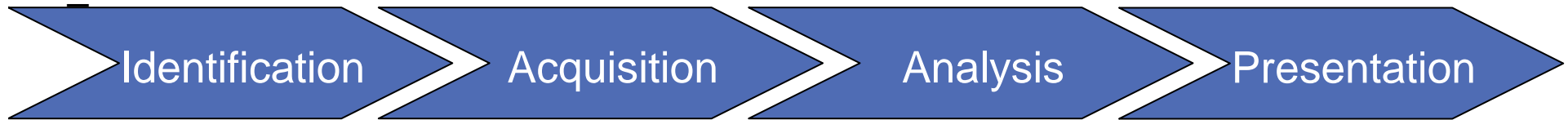
Hardware

2006 ACPI+PCI Firmware Demo
(Heasman)

Volatile memory forensics Potential evidence

- Loaded modules (DLL's)
- Running processes
- Network connections
- Open network ports
- Open files
- Dynamic Configuration
- **Hidden processes (Schuster)**
- **Terminated processes (Schuster)**
- **Cryptographic keys (Walters)**
- **Unencrypted content (Venema)**
- **Chat histories**
- ...

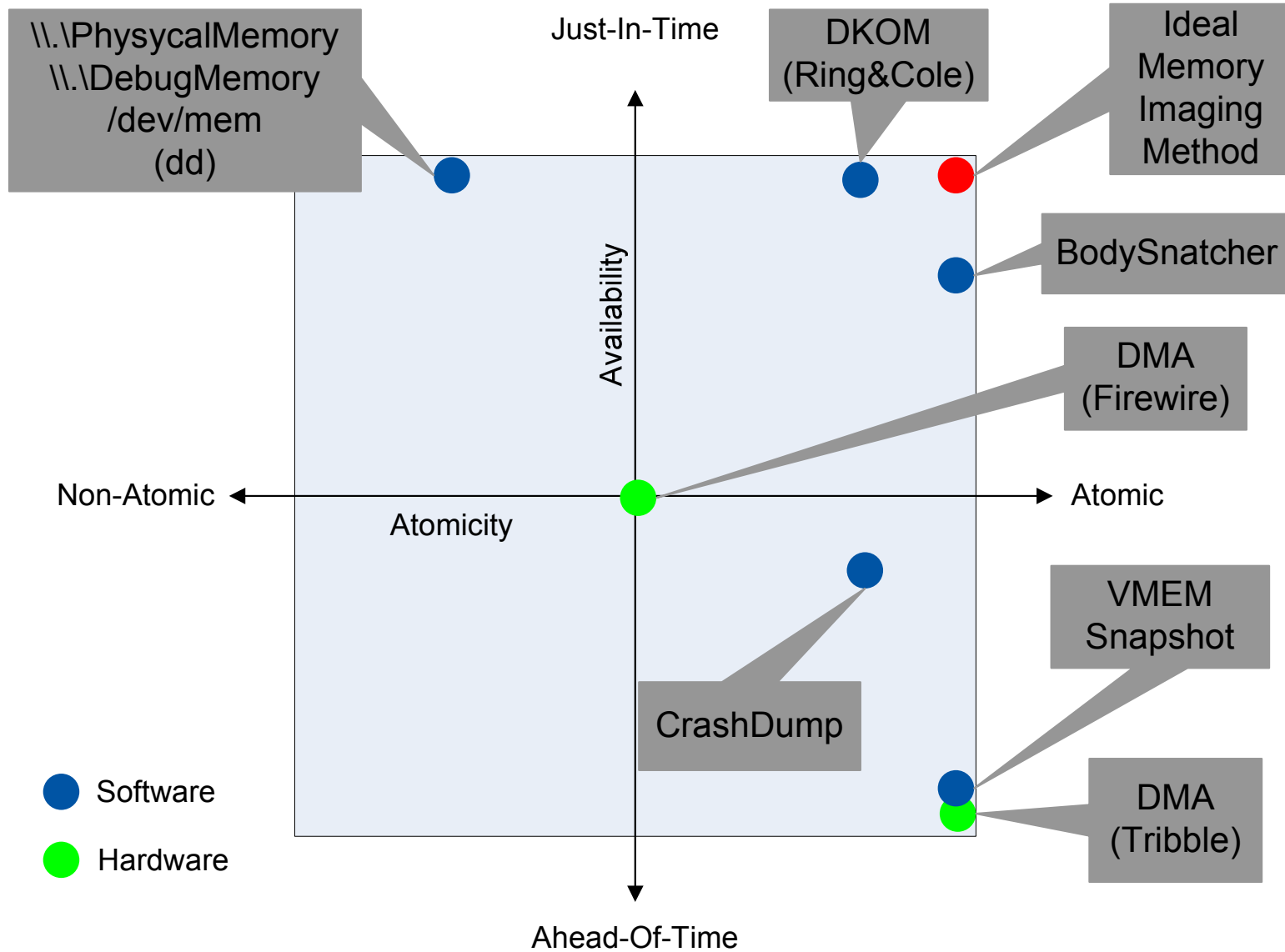




- Crime or misuse observed
- Identify potential evidence
- ***Volatile memory imaged***
- Live response performed
- Plug pulled
- Hard drive imaged
- Detailed analysis of image
- Reporting

Volatile memory forensics

Acquisition approaches



- dd
 - ~~Garner's dd~~
 - KntTools (Garner)
 - memimager (Vindstrom)
 - EnCase, etc
- DMA
 - Pythonraw1394 (Boileau)
- Crashdump
 - Notmyfault (Sysinternals)
 - Keyboard fault handler

- Text searching
 - Unix strings(1) (beware unicode issues)
 - Strings (Sysinternals)
 - Bintext (Foundstone)
- Binary Signature matching
 - PTfinder (Schuster)
 - DKOM resistant
 - Istools (Carvey)..

- Structural interpretation
 - Volatility (Walters)
 - KntTools (Garner)
 - WinDbg
 - Forensic extensions (Burdach)
 - Semantic integrity checking

Volatile memory forensics

Analysis example

```
C:\opt\Volatility-1.2.2pre>c:\Python25\python.exe volatility pslist -f helium.memdump
```

Name	Pid	PPid	Thds	Hnds	Time
System	4	0	98	1295	Thu Jan 01 00:00:00 1970
smss.exe	1104	4	3	21	wed Nov 28 07:36:18 2007
csrss.exe	1208	1104	12	958	wed Nov 28 07:36:22 2007
winlogon.exe	1232	1104	21	621	wed Nov 28 07:36:24 2007
services.exe	1276	1232	16	377	wed Nov 28 07:36:24 2007
lsass.exe	1288	1232	23	495	wed Nov 28 07:36:24 2007
ibmpmsvc.exe	1488	1276	5	38	wed Nov 28 07:36:26 2007
svchost.exe	1516	1276	23	232	wed Nov 28 07:36:26 2007
svchost.exe	1580	1276	12	434	wed Nov 28 07:36:26 2007
svchost.exe	1920	1276	90	2006	wed Nov 28 07:36:27 2007
svchost.exe	1972	1276	6	109	wed Nov 28 07:36:27 2007
svchost.exe	816	1276	17	311	wed Nov 28 07:36:28 2007
spoolsv.exe	1204	1276	10	145	wed Nov 28 07:36:28 2007
IPSSVC.EXE	1676	1276	94	240	wed Nov 28 07:36:28 2007
AcPrfMgrSvc.exe	1704	1276	7	99	wed Nov 28 07:36:28 2007
acs.exe	1756	1276	13	226	wed Nov 28 07:36:28 2007
svchost.exe	328	1276	4	77	wed Nov 28 07:36:29 2007
cvpnd.exe	1448	1276	3	126	wed Nov 28 07:36:29 2007
mdm.exe	1748	1276	5	85	wed Nov 28 07:36:30 2007
ntpd.exe	380	1276	5	100	wed Nov 28 07:36:30 2007
NTRtScan.exe	396	1276	15	122	wed Nov 28 07:36:30 2007
SMAgent.exe	688	1276	2	27	wed Nov 28 07:36:30 2007
svchost.exe	744	1276	7	125	wed Nov 28 07:36:30 2007
SUService.exe	776	1276	6	125	wed Nov 28 07:36:30 2007
TmListen.exe	1880	1276	13	194	wed Nov 28 07:36:30 2007
TPHDEXLG.exe	1900	1276	5	65	wed Nov 28 07:36:31 2007
TpKmpSvc.exe	1912	1276	2	23	wed Nov 28 07:36:31 2007
ibmtcsd.exe	2028	1276	3	40	wed Nov 28 07:36:31 2007
rrservice.exe	2040	1276	5	161	wed Nov 28 07:36:31 2007
tvtsched.exe	480	1276	5	108	wed Nov 28 07:36:31 2007
wdfmar.exe	724	1276	4	64	wed Nov 28 07:36:33 2007

```
C:\opt\volatility-1.2.2pre>c:\Python25\python.exe volatility connections -f helium.memdump
```

Local Address	Remote Address	Pid
127.0.0.1:1593	127.0.0.1:1594	5456
127.0.0.1:1595	127.0.0.1:1596	5456
127.0.0.1:1594	127.0.0.1:1593	5456
127.0.0.1:1596	127.0.0.1:1595	5456
10.0.50.106:1610	217.70.33.132:80	1684
10.0.50.106:1586	207.46.109.38:1863	5632
10.0.50.106:1660	72.14.253.91:80	5456
10.0.50.106:1620	150.101.98.69:80	5456
10.0.50.106:1616	150.101.98.69:80	5456
10.0.50.106:1628	150.101.98.72:80	5456
10.0.50.106:1636	150.101.98.70:80	5456
10.0.50.106:1648	150.101.98.70:80	2452
10.0.51.120:1547	10.0.51.10:445	816
10.0.50.106:1604	69.63.176.11:80	1684
10.0.50.106:1629	150.101.98.77:80	5456
10.0.50.106:1637	150.101.98.77:80	5456
10.0.50.106:1601	150.101.98.69:80	5456
10.0.50.106:1605	150.101.98.77:80	5456
10.0.50.106:1621	150.101.98.72:80	5456
10.0.50.106:1646	150.101.98.70:80	5192
10.0.50.106:1618	150.101.98.69:80	5456
10.0.50.106:1564	71.237.203.31:7145	4872
10.0.50.106:1623	150.101.98.77:80	5456
10.0.50.106:1619	150.101.98.69:80	5456
10.0.50.106:1627	150.101.98.72:80	5456
10.0.50.106:1631	150.101.98.69:80	5456
10.0.50.106:1615	150.101.98.69:80	5456

- Toolsets currently limited
- Acquisition approaches involve tradeoffs
- ? Anti-forensics
- ? Obtrusiveness

- Noise reduction – NSRL Hashset
- Further mapping of the kernel and userspace
- OS/Platforms

- *Widespread adoption*

- Volatility:
 - <http://www.volatilitysystems.com/VolatileWeb/volatility.gsp>
- KntTools
 - <http://www.gmgssystemsincc.com/knttools/>
- Andreas Schuster
 - <http://computer.forensikblog.de/en/>
- Harlan Carvey
 - <http://windowsir.blogspot.com/>
- Kesse Kornblum
 - <http://jessekornblum.livejournal.com/>
- Mariusz Burdach
 - <http://seccure.blogspot.com/>

Thank you!

bradley.schatz@evimetry.com.au