

# Visual Forensic Analysis and Reverse Engineering of Binary Data

*Gregory Conti*

*Erik Dean*

*United States Military Academy*

*West Point, New York*

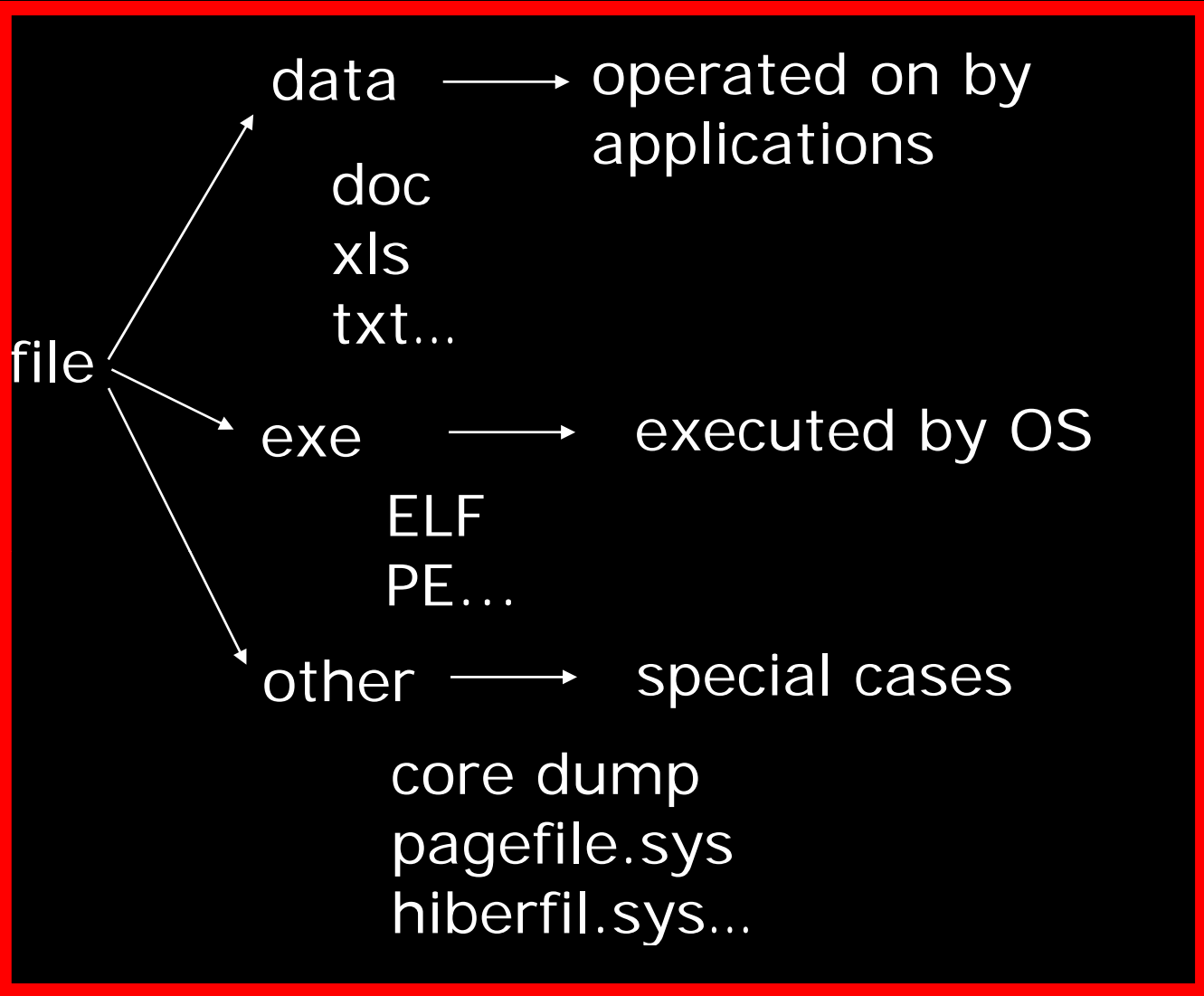
*gregory.conti@usma.edu*

*erik.dean@usma.edu*

# Outline

- The Problem – Tiny Windows
- Background and Motivation
- Related Work
- Moving Beyond Hex
- System Design
- Case Studies
- Demos

01010  
10101  
01010



memory process memory cache...  
network packets...

high  
insight

Ida Pro  
OllyDBG  
BinNavi (Zynamics)  
BinDiff (Zynamics)...

Filemon  
Regmon...

lower  
insight

011

hex editors  
hexdump  
grep & diff  
strings

objdump

original  
application

general purpose

precise application

# strings /grep/diff

```
H:\Datasets>strings 20040517_homeISP.pcap | more
```

```
Strings v2.4
```

```
Copyright (C) 1999-2007 Mark Russinovich
```

```
Sysinternals - www.sysinternals.com
```

```
0hF
```

```
M@y
```

```
7bs
```

```
Z19Z
```

```
MICROSOFT NETWORKS
```

```
WINDOWS USER
```

```
Microsoft Security Bulletin MS03-043
```

```
Buffer Overrun in Messenger Service Could Allow Code Execution  
(828035)
```

```
Affected Software:
```

```
Microsoft Windows NT Workstation
```

```
Microsoft Windows NT Server 4.0
```

```
Microsoft Windows 2000
```

```
...
```

# 011 Hex Editor

The screenshot displays the 010 Editor application window. The title bar reads "010 Editor - C:\Documents and Settings\dg1157\Desktop\Giant Demo\INSECURE-Mag-15.pdf". The menu bar includes File, Edit, Search, View, Scripts, Templates, Tools, Window, and Help. The toolbar contains various icons for file operations and editing. The "Edit As:" dropdown is set to "Hex".

The main workspace is divided into three panes:

- Workspace:** Shows a tree view with "Open Files" containing "C:\...Giant Demo\INSECURE-Mag-15.pdf", "Favorite Files", "Recent Files", and "Bookmarked Files".
- Inspector:** A table showing data types and their values. The current value is a string: "%PDF-1.5 0 obj <<...".
- Main Editor:** A hex editor view for "INSECURE-Mag-15.pdf". It shows a grid of hex bytes (0000h to 01F0h) and their corresponding ASCII characters. The first few lines of the PDF header are visible: "%PDF-1.5 0 obj", "<<./Length 120", and "/Filter /".

The status bar at the bottom indicates: "Opened file 'C:\Documents and Settings\dg1157\Desktop\Giant Demo\INSECURE-Mag-15.pdf'. Pos: 0 [0h] Val: 37 25h 00100101b Size: 11780393 ANSI LIT W OVR".

# Hex Workshop

The screenshot displays the Hex Workshop interface with the following components:

- Hex Dump:** A grid showing hexadecimal values and their corresponding ASCII characters. The ASCII column contains PDF metadata such as `%PDF-1.5`, `obj <<./L`, `ength 120`, `./Filt`, `er /FlateDecode.>>.str`, `eam.x...M...@...s...L`, `t<@A...\.2...t.N..A.H.`, `...e(...3.k.\(...*R.`, `..P...p...Jy~.;H..`, `D3.i..Sz... K.....4.{.Y`, `.U...M^...4.endstrea`, `m.endobj.3 0 obj <<./T`, `ype /Page./Contents 4`, `0 R./Resources 2 0 R./`, `MediaBox [0 0 594.989`, `841.978]./Parent 5 0 R`, `.>> endobj.1 0 obj <<.`, `/Type /XObject./Subtyp`, `e /Form./FormType 1./P`, `TEX.FileName (/tmp/pdf`, `lab/tempfile0.pdf)./PT`, `EX.PageNumber 1./PTEX.`, `InfoDict 6 0 R ./Matri`, `x [1.00000000 0.000000`, `00 0.00000000 1.000000`, `00 0 00000000 0 000000`
- Data Inspector:** Located at the bottom left, it shows a list of data types and their values for the selected offset (184).

Offset: 184 [0x000000B8]	Value
8BIT Signed Byte	-32
8BIT Unsigned Byte	224
16BIT Signed Short	3040
16BIT Unsigned Short	3040
32BIT Signed Long	365235168
32BIT Unsigned Long	365235168
64BIT Signed Quad	7954926168732666848
64BIT Unsigned Quad	7954926168732666848
32BIT Float	7.9586402e-026
- Compare Results:** Located at the bottom right, it shows a table for comparing source and target values.

Source	Count	Count	Target	Count
--------	-------	-------	--------	-------
- Status Bar:** At the bottom, it displays `Ready`, `Offset: 000000B8`, `Value: 3040`, `11780393 bytes`, and `OVF MOD READ`.

# WinHex

The screenshot displays the WinHex application window titled "WinHex - [Drive H:]". The interface includes a menu bar (File, Edit, Search, Position, View, Tools, Specialist, Options, File Manager, Window, Help) and a toolbar. A file explorer on the left shows the directory structure of drive H:\, including folders like "Common Files", "CyberLink", and "MSN Gaming Zone". The "Tools" menu is open, showing options such as "Disk Tools", "RAM Editor...", "Invoke Text Editor", "Invoke Viewer", "Calculator", "Hex Converter...", "Analyze Block", "Calculate Hash...", and "Start Center...". A sub-menu for "Disk Tools" is also visible, containing options like "List Clusters...", "Re-Scan Cluster Chains", "Initialize Free Space...", "Initialize SJack Space...", "Initialize MFT Records...", "Clone Disk...", "File Recovery by Name...", "File Recovery by Type...", "Interpret File As Disk", and "Set Disk Parameters...".

The main window is divided into several panes. The top right pane shows drive information for Drive H: (53% free, NTFS, original state). The middle right pane displays a file list with columns for "Access" and "Attr.". The bottom right pane shows disk statistics: Bytes per cluster (4,096), Free clusters (555,455), Total clusters (1,050,241), Bytes per sector (512), and Total no. of sectors (8,401,928). The bottom right pane also shows "Last scanned: 1 min. ago", "Cluster No.: 972952", and "Program Files H:\".

The central pane is a hex editor showing a table of hex values and their ASCII representations. The table has columns for "Offset" (0 to F) and "Access". The hex values are: 0ED898000: 49 4E 44 58 28 00 09 00 A8 7B 1F 49 00 00 00 00; 0ED898010: 00 00 00 00 00 00 00 00 28 00 00 00 E0 05 00 00; 0ED898020: E8 0F 00 00 00 00 00 00 4B 00 01 00 C2 01 72 00; 0ED898030: 00 00 00 00 C2 01 73 00 00 00 00 00 00 00 00 00; 0ED898040: 7C 0D 00 00 00 00 05 7C 70 00 5A 00 00 00 00 00; 0ED898050: 7B 0D 00 00 00 00 01 00 90 C4 A1 6D AA 4B C2 01; 0ED898060: 90 64 AF EB 87 0A C3 01 90 64 AF EB 87 0A C3 01; 0ED898070: 90 64 AF EB 87 0A C3 01 00 00 00 00 00 00 00 00; 0ED898080: 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00; 0ED898090: 0C 01 43 00 6F 00 6D 00 6D 00 6F 00 6E 00 20 00; 0ED8980A0: 46 00 69 00 6C 00 65 00 73 00 00 00 00 00 00 00; 0ED8980B0: 7C 0D 00 00 00 00 05 7C 68 00 52 00 00 00 00 00; 0ED8980C0: 7B 0D 00 00 00 00 01 00 90 C4 A1 6D AA 4B C2 01; 0ED8980D0: 90 64 AF EB 87 0A C3 01 90 64 AF EB 87 0A C3 01; 0ED8980E0: 90 64 AF EB 87 0A C3 01 00 00 00 00 00 00 00 00; 0ED8980F0: 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00; 0ED898100: 08 02 43 00 4F 00 4D 00 4D 00 4F 00 4E 00 7E 00.

The bottom status bar shows "Sector 7783616 of 8401928", "Offset: ED898000", "= 73", "Block: ED898092 - ED8980A9", and "Size: 18". A "Data Interpreter" dialog box is open in the bottom right corner, showing options for "8 Bit (±) 73", "16 Bit (±) 20041", and "32 Bit (±) 1480871497".



high  
insight

Ida Pro  
OllyDBG  
BinNavi (Zynamics)  
BinDiff (Zynamics)...

Filemon  
Regmon...

lower  
insight

011

hex editors  
hexdump  
grep & diff  
strings

objdump  
  
original  
application

general purpose

precise application

high  
insight

Ida Pro  
OllyDBG  
BinNavi (Zynamics)  
BinDiff (Zynamics)...

Filemon  
Regmon...

lower  
insight

011

hex editors  
hexdump  
grep & diff  
strings

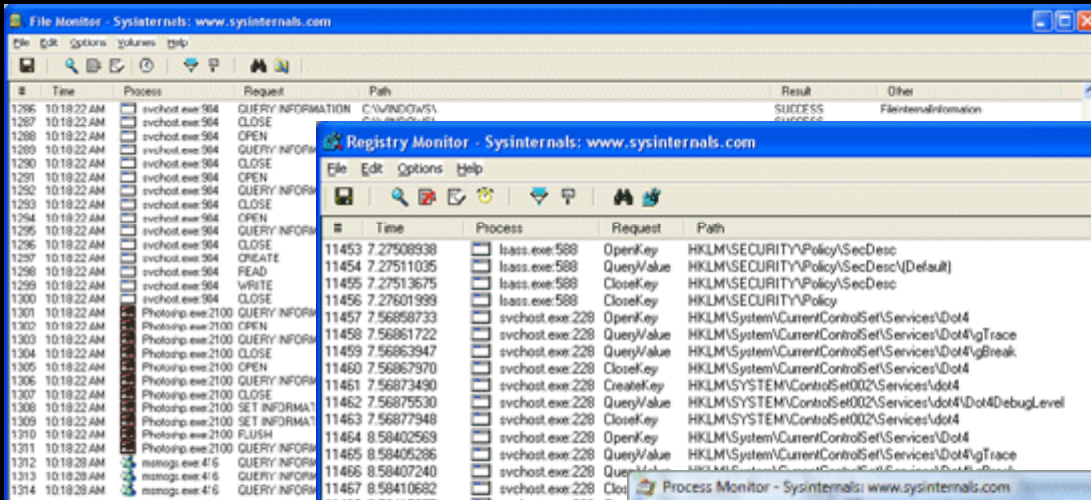
objdump

original  
application

general purpose

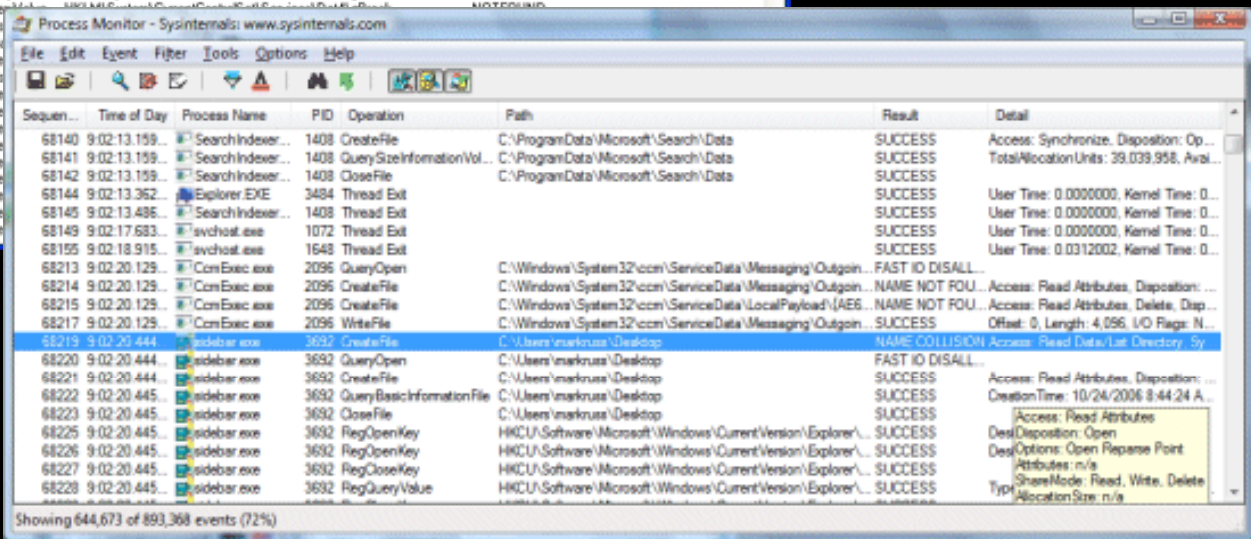
precise application

# SysInternals



FileMon

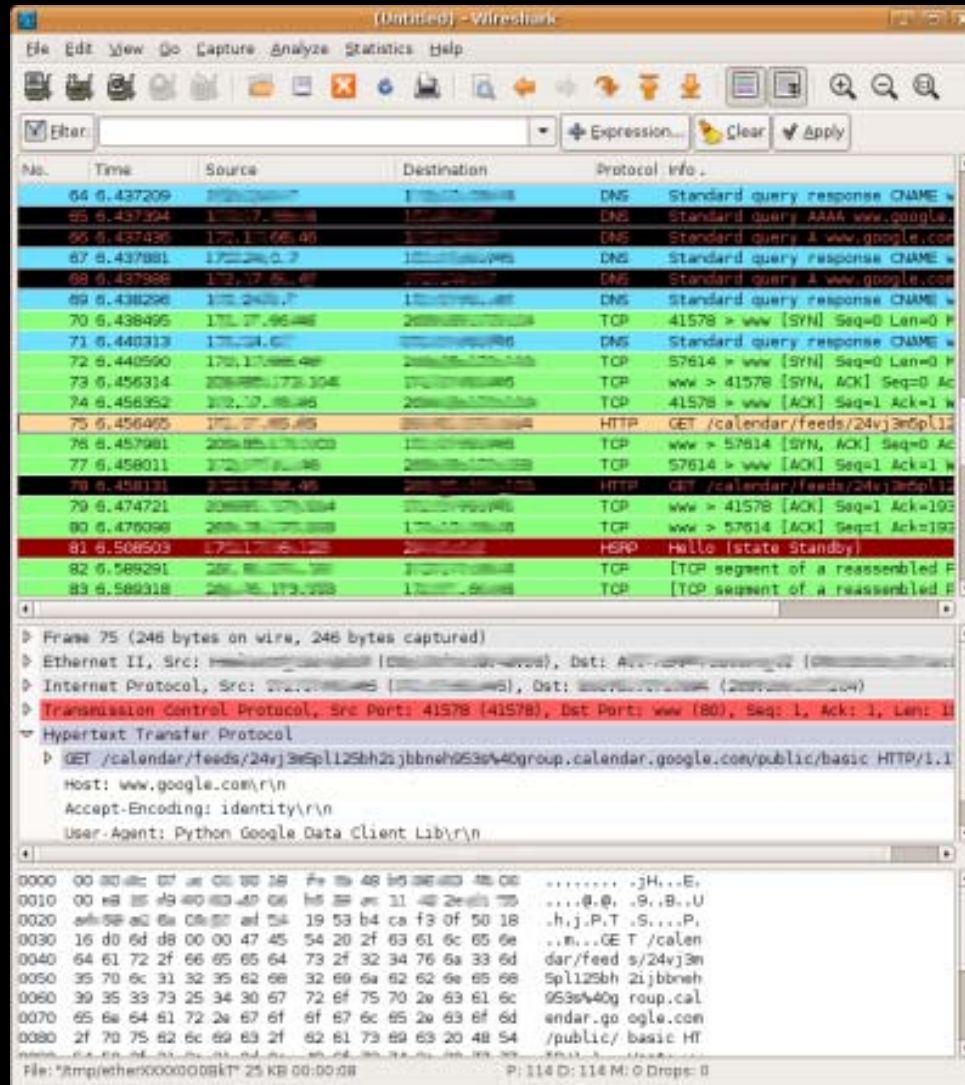
RegMon



Process Monitor

...

# Wireshark



# OllyDbg

The screenshot displays the OllyDbg interface for the process NOTEPAD.EXE. The CPU window shows the main thread at address 010016A4, with registers like EAX (00000000), ECX (0007FFB0), and EIP (01007390). The disassembly window shows instructions such as CHAR '\', CHAR 'P', and CHAR 'T'. The memory dump window shows hex dump and ASCII values for the current instruction. The status bar at the bottom indicates 'Analysing NOTEPAD: 77 heuristical procedures, 516 calls to known, 151 calls to guessed functions' and a 'Paused' button.

**Registers (FPU)**

EAX	00000000
ECX	0007FFB0
EDX	7C90E894 ntdll.KiFastSystemCallRet
EBX	7FFDA000
ESP	0007FFC4
EBP	0007FFB0
ESI	FFFFFFFF
EDI	7C910738 ntdll.7C910738
EIP	01007390 NOTEPAD.<ModuleEntryPoint>

**Disassembly**

Address	Hex dump	ASCII
010016A4	53 00 6F 00 66 00	Unicode "Software"
010016A8	5C 00 4D 00 69 00	Unicode "Microsof"
010016AC	66 00 74 00 5D 00	Unicode "r\notep"
010016B0	61 00 64 00 00 00	Unicode "ad",0
010016B4	00 00 00 00	DB 00
010016B8	40 00 75 00 63 00	Unicode "Lucida C"
010016BC	6F 00 6E 00 73 00	Unicode "onsole",0
010016C0	00 00 00 00	DB 00
010016C4	4F 00 75 00 74 00	Unicode "Out of R"
010016C8	43 00 29 00 73 00	Unicode "C string"
010016CC	20 00 73 00 70 00	Unicode " space!"
010016D0	00 00 00 00	Unicode 0
010016D4	00 00 00 00	DB 00
010016D8	44 00 45 00 56 00	Unicode "DEV Erro"
010016DC	72 00 21 00 00 00	Unicode "r!",0
010016E0	00 00 00 00	DB 00
010016E4	53 00 6C 00 69 00	Unicode "SlipUpAc"
010016E8	63 00 00 00	Unicode "c",0
010016EC	2F 00 2E 00 53 00	Unicode ".,SETUP",0
010016F0	00 00 00 00	DB 00
010016F4	50 00 00 00	DB 50
010016F8	00 00 00 00	DB 00
01001700	00 00 00 00	DB 00
01001704	00 00 00 00	DB 00
01001708	00 00 00 00	DB 00
0100170C	00 00 00 00	DB 00
01001710	00 00 00 00	DB 00
01001714	00 00 00 00	DB 00
01001718	00 00 00 00	DB 00
0100171C	00 00 00 00	DB 00
01001720	00 00 00 00	DB 00
01001724	00 00 00 00	DB 00
01001728	00 00 00 00	DB 00
0100172C	00 00 00 00	DB 00
01001730	00 00 00 00	DB 00
01001734	00 00 00 00	DB 00
01001738	00 00 00 00	DB 00
0100173C	00 00 00 00	DB 00
01001740	00 00 00 00	DB 00
01001744	00 00 00 00	DB 00
01001748	00 00 00 00	DB 00
0100174C	00 00 00 00	DB 00
01001750	00 00 00 00	DB 00
01001754	00 00 00 00	DB 00
01001758	00 00 00 00	DB 00
0100175C	00 00 00 00	DB 00
01001760	00 00 00 00	DB 00
01001764	00 00 00 00	DB 00
01001768	00 00 00 00	DB 00
0100176C	00 00 00 00	DB 00
01001770	00 00 00 00	DB 00
01001774	00 00 00 00	DB 00
01001778	00 00 00 00	DB 00
0100177C	00 00 00 00	DB 00
01001780	00 00 00 00	DB 00
01001784	00 00 00 00	DB 00
01001788	00 00 00 00	DB 00
0100178C	00 00 00 00	DB 00
01001790	00 00 00 00	DB 00
01001794	00 00 00 00	DB 00
01001798	00 00 00 00	DB 00
0100179C	00 00 00 00	DB 00
010017A0	00 00 00 00	DB 00
010017A4	00 00 00 00	DB 00
010017A8	00 00 00 00	DB 00
010017AC	00 00 00 00	DB 00
010017B0	00 00 00 00	DB 00
010017B4	00 00 00 00	DB 00
010017B8	00 00 00 00	DB 00
010017BC	00 00 00 00	DB 00
010017C0	00 00 00 00	DB 00
010017C4	00 00 00 00	DB 00
010017C8	00 00 00 00	DB 00
010017CC	00 00 00 00	DB 00
010017D0	00 00 00 00	DB 00
010017D4	00 00 00 00	DB 00
010017D8	00 00 00 00	DB 00
010017DC	00 00 00 00	DB 00
010017E0	00 00 00 00	DB 00
010017E4	00 00 00 00	DB 00
010017E8	00 00 00 00	DB 00
010017EC	00 00 00 00	DB 00
010017F0	00 00 00 00	DB 00
010017F4	00 00 00 00	DB 00
010017F8	00 00 00 00	DB 00
010017FC	00 00 00 00	DB 00

**Memory Dump**

Address	Hex dump	ASCII
01009000	00 00 00 00 04 70 00 01	....f0.0
01009004	00 00 00 00 00 00 00 00	.....
01009008	00 00 00 00 00 00 00 00	.....
0100900C	73 00 00 00 01 00 00 00	x...0...
01009010	4E 00 6F 00 74 00 65 00	N.o.t.e
01009014	70 00 61 00 64 00 00 00	p.a.d....
01009018	FF FF FF FF 01 00 00 00	0....
0100901C	02 00 00 00 03 00 00 00	0...0...
01009020	04 00 00 00 05 00 00 00	0...0...
01009024	06 00 00 00 07 00 00 00	0...0...
01009028	08 00 00 00 09 00 00 00	0...0...
0100902C	0A 00 00 00 0B 00 00 00	0...0...
01009030	0C 00 00 00 0D 00 00 00	0...0...
01009034	0E 00 00 00 0F 00 00 00	0...0...
01009038	10 00 00 00 11 00 00 00	0...0...
0100903C	12 00 00 00 13 00 00 00	0...0...
01009040	14 00 00 00 15 00 00 00	0...0...
01009044	16 00 00 00 17 00 00 00	0...0...
01009048	18 00 00 00 19 00 00 00	0...0...
0100904C	1A 00 00 00 1B 00 00 00	0...0...
01009050	1C 00 00 00 1D 00 00 00	0...0...
01009054	1E 00 00 00 1F 00 00 00	0...0...
01009058	20 00 00 00 21 00 00 00	0...0...
0100905C	22 00 00 00 23 00 00 00	0...0...
01009060	24 00 00 00 25 00 00 00	0...0...
01009064	26 00 00 00 27 00 00 00	0...0...
01009068	28 00 00 00 29 00 00 00	0...0...
0100906C	2A 00 00 00 2B 00 00 00	0...0...
01009070	2C 00 00 00 2D 00 00 00	0...0...
01009074	2E 00 00 00 2F 00 00 00	0...0...
01009078	30 00 00 01 38 00 00 01	4E.08E.0
0100907C	3C 00 00 01 40 00 00 01	<E.08E.0
01009080	4C 00 00 01 48 00 00 01	LE.08E.0

Analysing NOTEPAD: 77 heuristical procedures, 516 calls to known, 151 calls to guessed functions

Paused

# IDA Pro

v5.1

The screenshot displays the IDA Pro v5.1 interface with several key components highlighted by red boxes:

- Assembly View:** Shows assembly instructions for a function. The highlighted code includes:

```
mov [ebp+var_38], eax
push offset ___xc_2
call _initterm
add esp, 2Ah
mov eax, ds: _imp___accdin
mov esi, [eax]
mov [ebp+var_20], esi
cmp byte ptr [esi], 22h
inc short loc_1007AF7
```
- Control Flow Graph (CFG):** A graph showing the flow of execution between basic blocks. The highlighted blocks include:
  - `loc_1007A80`:

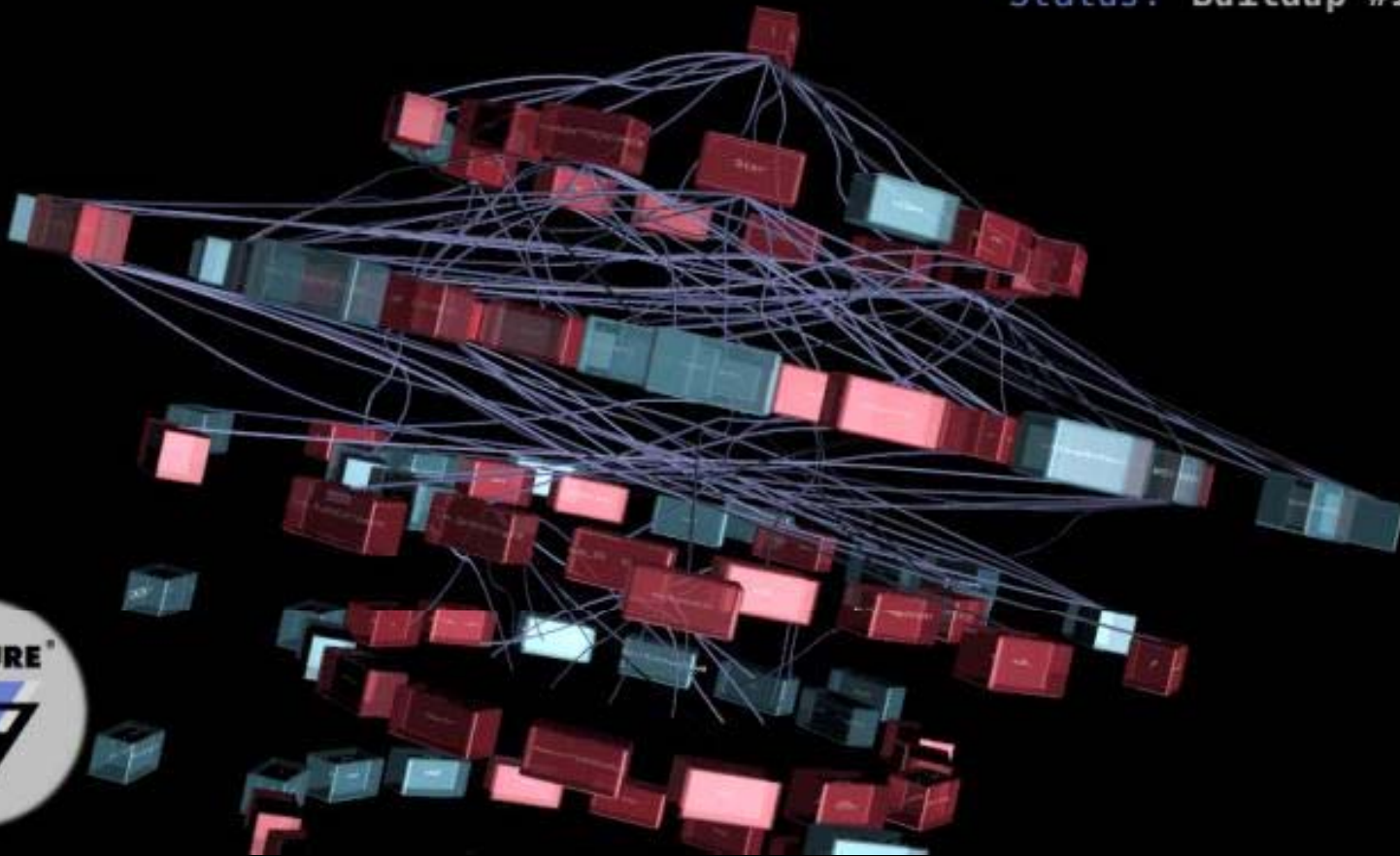
```
inc esi
mov [ebp+var_20], esi
mov al, [esi]
cmp al, bl
jz short loc_1007ACB
```
  - `loc_1007AF7`:

```
inc esi
mov [ebp+var_20], esi
jnp short loc_1007AF7
```
  - `loc_1007ACB`:

```
cmp byte ptr [esi], 22h
inc short loc_1007A80
```
- Hex View:** Displays the raw hex data corresponding to the assembly instructions, with a hex-to-ascii conversion window open above it.
- Names Window:** Lists various symbols and functions, such as `__recalc_check_coubin()`, `__report_grabax`, and `__set_abortProc`.
- Structures Window:** Shows a list of structures defined in the program, including `__set_abortProc`, `__set_abortProc`, and `__set_abortProc`.

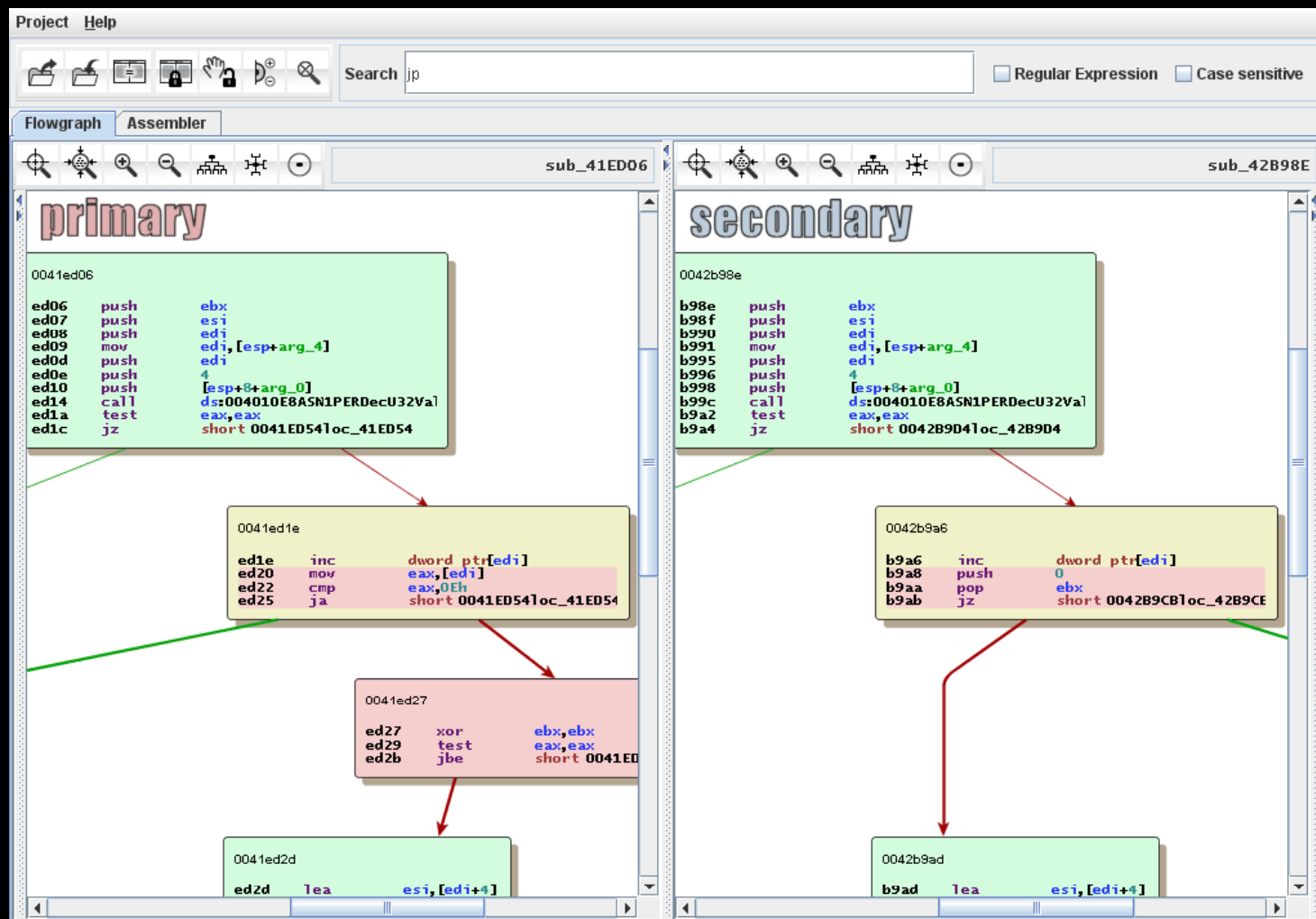
# F-Secure Malware

Sample: W32/Bagle.AG@mm  
Status: Buildup #1



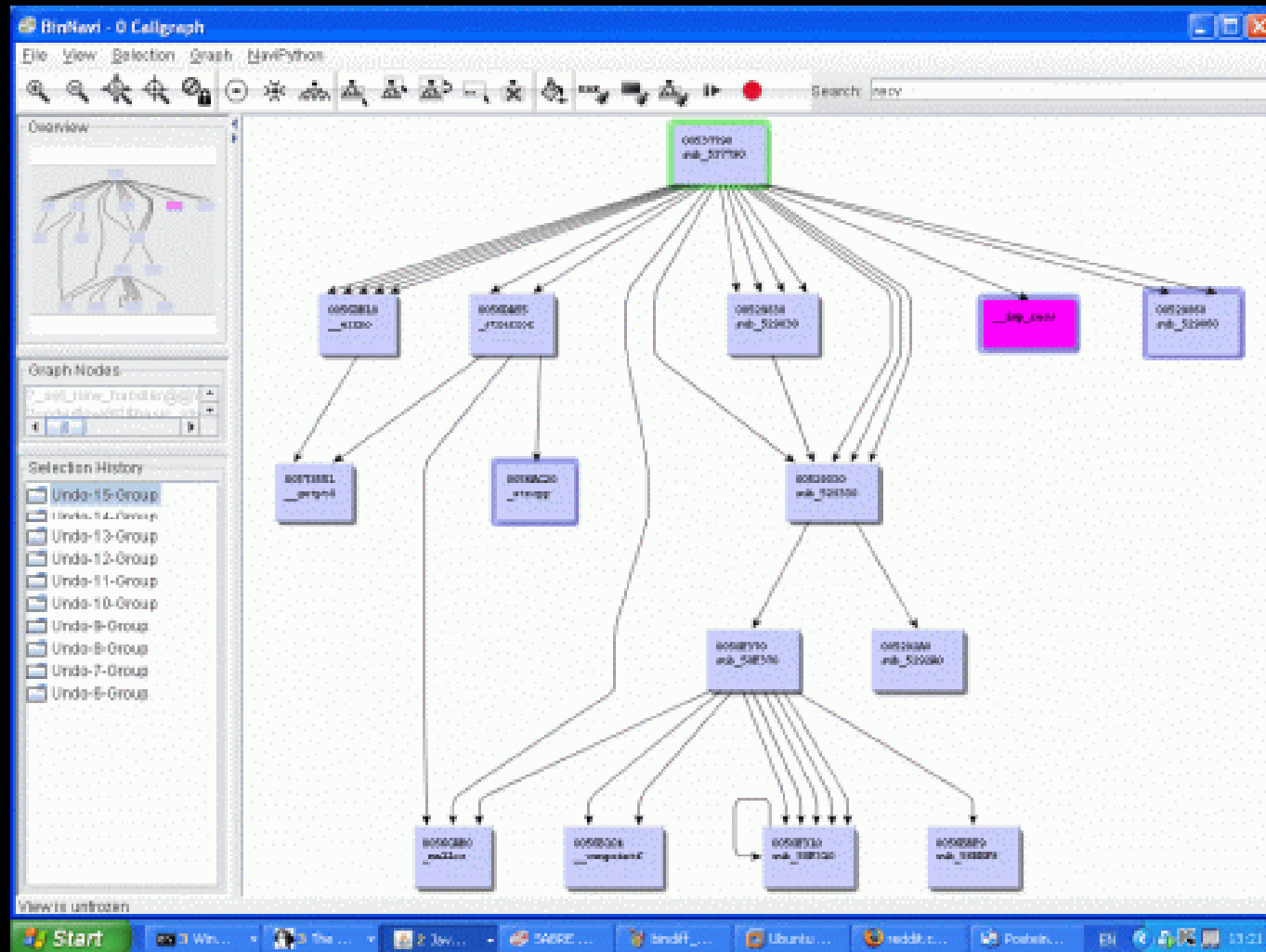
<http://www.f-secure.com/weblog/archives/00000662.html>

# Zynamics BinDiff





# Zynamics BinNavi



high  
insight

Ida Pro  
OllyDBG  
BinNavi (Zynamics)  
BinDiff (Zynamics)...

Filemon  
Regmon...

lower  
insight

011

hex editors  
hexdump  
grep & diff  
strings

objdump

original  
application

general purpose

precise application

# Framework

- File Independent Level
  - Entropy
  - Byte Frequency
  - N-Gram Analysis
  - Strings
  - Hex / Decimal / ASCII
  - Bit Plot (2D/3D)
  - File Statistics
- File Specific Level
  - Complete or Partial Knowledge of File Structure
  - For Example, Metadata

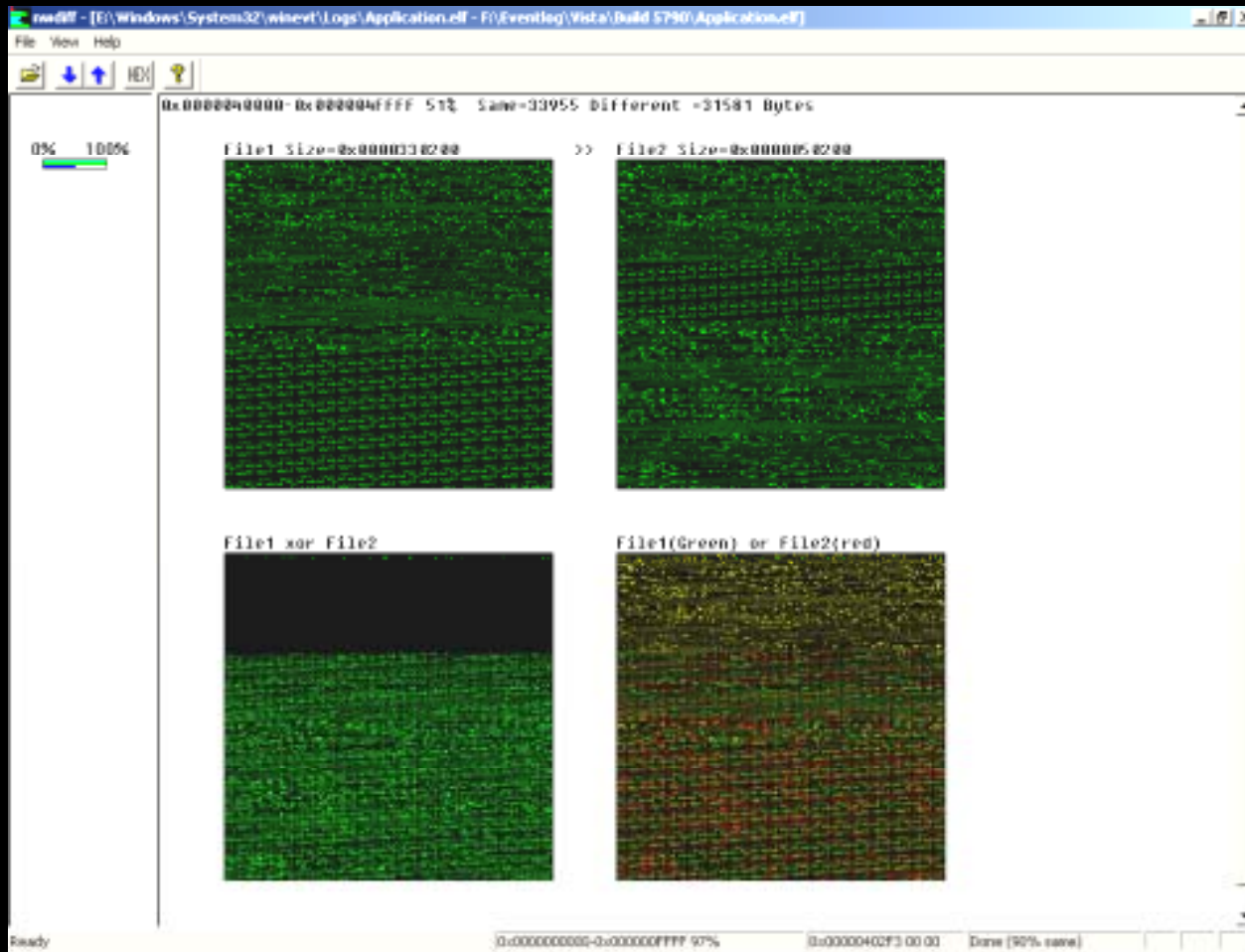
# Syntax Highlighting for Hex Dumps

(Kaminsky)

```
4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e8 00 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68
69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a
24 00 00 00 00 00 00 00 00 00 ce 0d 2d e1 8a 6c 43 b2 8a 6c 43 b2 8a 6c 43 b2 49 63 1e b2 04 6c 43 b2 8a 6c 42 b2 de 6c 43 b2
49 63 4c b2 dd 6c 43 b2 49 63 1d b2 8b 6c 43 b2 49 63 1c b2 0c 6e 43 b2 49 63 1f b2 8b 6c 43 b2 49 63 19 b2 8b 6c 43 b2
52 69 63 68 8a 6c 43 b2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 15 00
f9 0f 25 42 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 07 0a 00 05 1c 00 80 36 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 a2 06 00 00 00 00 40 00 80 00 00 00 80 00 00 00 05 00 01 00 05 00 01 00 05 00 01 00 05 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
af 98 21 00 01 00 00 00 00 00 04 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00
e4 36 1f 00 50 00 00 00 00 00 40 1f 00 08 07 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
c0 1c 07 00 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 80 05 00 00 54 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
2e 74 65 78 74 00 00 00 a1 17 07 00 80 05 00 00 00 18 07 00 80 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
50 4f 4f 4c 4d 49 00 00 00 b3 12 00 00 80 1d 07 00 00 13 00 00 80 1d 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
4d 49 53 59 53 50 54 45 00 07 00 00 80 30 07 00 00 07 00 00 80 30 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
50 4f 4f 4c 43 4f 44 45 a0 15 00 00 80 37 07 00 00 16 00 00 80 37 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
2e 64 61 74 61 00 00 00 a0 6c 01 00 80 4d 07 00 00 6d 01 00 80 4d 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
50 41 47 45 00 00 00 00 24 8d 0f 00 80 ba 08 00 80 8d 0f 00 80 ba 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
50 41 47 45 4c 4b 00 00 62 e3 00 00 00 48 18 00 80 e3 00 00 00 48 18 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
50 41 47 45 56 52 46 59 cd f1 00 00 80 2b 19 00 00 f2 00 00 80 2b 19 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
50 41 47 45 57 4d 49 00 f2 17 00 00 80 1d 1a 00 00 18 00 00 80 1d 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
50 41 47 45 4b 44 00 00 52 40 00 00 80 35 1a 00 00 40 00 00 80 35 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
50 41 47 45 53 50 45 43 43 0c 00 00 00 00 76 1a 00 80 0c 00 00 00 76 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
50 41 47 45 48 44 4c 53 d8 1d 00 00 80 82 1a 00 00 1e 00 00 80 82 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
2e 65 64 61 74 61 00 00 0a b5 00 00 80 a0 1a 00 80 b5 00 00 80 a0 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
50 41 47 45 44 41 54 41 58 15 00 00 00 56 1b 00 80 15 00 00 00 56 1b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
50 41 47 45 4b 44 00 00 21 c0 00 00 80 6b 1b 00 80 c0 00 00 80 6b 1b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
50 41 47 45 43 4f 4e 53 8c 01 00 00 00 2c 1c 00 00 02 00 00 00 2c 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
50 41 47 45 56 52 46 43 49 34 00 00 00 2e 1c 00 80 34 00 00 00 2e 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
50 41 47 45 56 52 46 44 48 06 00 00 80 62 1c 00 80 06 00 00 80 62 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
49 4e 49 54 00 00 00 00 e8 46 02 00 00 69 1c 00 00 d7 02 00 00 69 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
2e 72 73 72 63 00 00 00 08 07 01 00 00 40 1f 00 80 07 01 00 00 40 1f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
2e 72 65 6c 6f 63 00 00 4c f9 00 00 80 47 20 00 80 f9 00 00 80 47 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 a8 38 1f 00 b8 38 1f 00 cc 38 1f 00 de 38 1f 00 f2 38 1f 00 fe 38 1f 00 16 39 1f 00 2e 39 1f 00 40 39 1f 00 5e 39 1f 00 7e 39 1f 00 98 39 1f 00 b0 39 1f 00 cc 39 1f 00 e8 39 1f 00 02 3a 1f 00
16 3a 1f 00 2a 3a 1f 00 42 3a 1f 00 5a 3a 1f 00 7e 3a 1f 00 8c 3a 1f 00 9e 3a 1f 00 ba 3a 1f 00 c4 3a 1f 00 d8 3a 1f 00 e4 3a 1f 00 f2 3a 1f 00 00 3b 1f 00 10 3b 1f 00 20 3b 1f 00 30 3b 1f 00
ec 3a 1f 00 00 3b 1f 00 1a 3b 1f 00 3c 3b 1f 00 52 3b 1f 00 62 3b 1f 00 7c 3b 1f 00 84 3b 1f 00 9e 3b 1f 00 ae 3b 1f 00 dc 3b 1f 00 ee 3b 1f 00 fe 3b 1f 00 00 3c 1f 00 10 3c 1f 00 20 3c 1f 00
ec 3b 1f 00 00 3c 1f 00 24 3c 1f 00 32 3c 1f 00 40 3c 1f 00 5c 3c 1f 00 70 3c 1f 00 84 3c 1f 00 9e 3c 1f 00 ae 3c 1f 00 be 3c 1f 00 ce 3c 1f 00 de 3c 1f 00 ee 3c 1f 00 fe 3c 1f 00 00 3d 1f 00
d4 3c 1f 00 e8 3c 1f 00 fc 3c 1f 00 0c 3d 1f 00 22 3d 1f 00 3a 3d 1f 00 52 3d 1f 00 68 3d 1f 00 82 3d 1f 00 9c 3d 1f 00 b4 3d 1f 00 c4 3d 1f 00 d4 3d 1f 00 e4 3d 1f 00
b2 3d 1f 00 c8 3d 1f 00 e4 3d 1f 00 0c 3e 1f 00 2a 3e 1f 00 3e 3e 1f 00 56 3e 1f 00 7a 3e 1f 00 9a 3e 1f 00 ba 3e 1f 00 da 3e 1f 00 ea 3e 1f 00 fa 3e 1f 00 00 3f 1f 00
b2 3e 1f 00 c8 3e 1f 00 e0 3e 1f 00 00 3f 1f 00 0e 3f 1f 00 2a 3f 1f 00 42 3f 1f 00 5e 3f 1f 00 72 3f 1f 00 8e 3f 1f 00 a2 3f 1f 00 b6 3f 1f 00 c2 3f 1f 00 d2 3f 1f 00 e2 3f 1f 00
80 3f 1f 00 8c 3f 1f 00 9e 3f 1f 00 b6 3f 1f 00 c0 3f 1f 00 d8 3f 1f 00 00 00 00 00 00 00 d8 06 40 00 00 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10
```

image: Dan Kaminsky, CCC2006

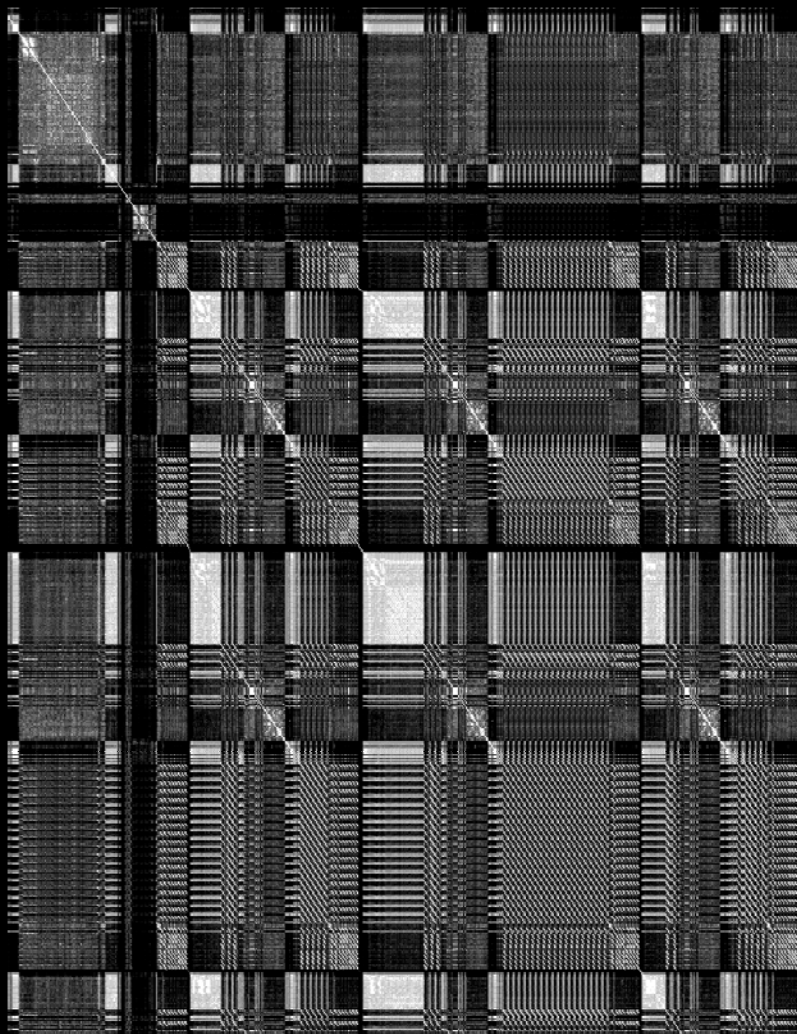
# nwdiff



[http://computer.forensikblog.de/en/2006/02/compare\\_binary\\_files\\_with\\_nwdiff.html](http://computer.forensikblog.de/en/2006/02/compare_binary_files_with_nwdiff.html)  
[http://www.geocities.jp/belden\\_dr/ToolNwdiff\\_Eng.html](http://www.geocities.jp/belden_dr/ToolNwdiff_Eng.html)

# Dot Plots & Visual BinDiff

(Kaminsky)



Self-Similarity in  
a single file. (.NET Assembly)



Diffing Two Files

Textual  
Hex/ASCII  
Detail View

Traditional  
Textual  
Utilities  
(strings...)

Graphical  
Displays

Machine Assisted Mapping and Navigation

Hex Editor Core

# Towards a Visual Hex Editor

- Identify Unknown Binaries
- Malware Analysis
- Analyze Unknown/Undocumented File Format
- Locate Embedded Objects
  - Encoding / Encryption
- Audit Files for Vulnerabilities
- Compare files (Diffing)
- Cracking
- Cryptanalysis
- Perform Forensic Analysis
- File System Analysis
- Reporting
- File Fuzzing



# Goals

- Handle Large Files
- Many Insightful Windows
- Big Picture Context
- Improved Navigation
- Data Files / Executable Files
- Hex Editor best practices is the foundation
- Support Art & Science

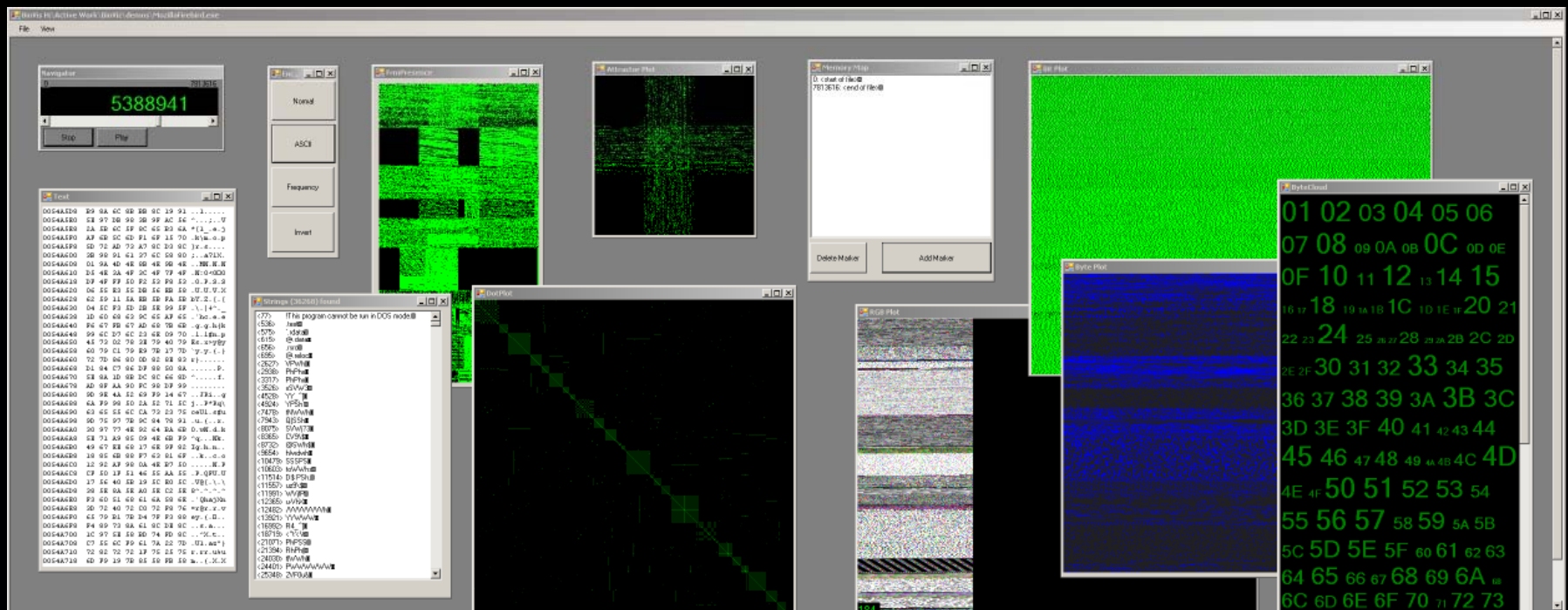
# Design

- Robust extensible framework
- Open source
- Context Independent File Analysis
- Semantic File Analysis
- Useful
- Multiple coordinated views
- Combine Functionality of current tools and extend with visuals

# Filtering + Encoding

- Identifying something
  - REGEX → algorithmic
- Using this knowledge to..
  - highlight
  - fade
  - remove
- Interactive or automated





- **Textual:** Text/ASCII, Strings, ByteCloud
- **Graphical:** Bitplot, BytePlot, RGBPlot, BytePresence, ByteFrequency, Digram, Dotplot
- **Interaction:** VCR, Memory Map, Color Coding

# Traditional Views

```
00000000 4D 5A 90 00 03 00 00 00 MZ.....
00000008 04 00 00 00 FF FF 00 00 .....
00000010 B8 00 00 00 00 00 00 00 .....
00000018 40 00 00 00 00 00 00 00 @.....
00000020 00 00 00 00 00 00 00 00 .....
00000028 00 00 00 00 00 00 00 00 .....
00000030 00 00 00 00 00 00 00 00 .....
00000038 00 00 00 00 20 01 00 00 .....
00000040 0E 1F BA 0E 00 B4 09 CD .....
00000048 21 B8 01 4C CD 21 54 68 !..L.!Th
00000050 69 73 20 70 72 6F 67 72 is progr
00000058 61 6D 20 63 61 6E 6E 6F am canno
00000060 74 20 62 65 20 72 75 6E t be run
00000068 20 69 6E 20 44 4F 53 20 in DOS
00000070 6D 6F 64 65 2E 0D 0A mode....
00000078 24 00 00 00 00 00 00 00 $......
00000080 D8 D4 07 F5 9C B5 69 A6 ..b...i.
00000088 9C B5 69 A6 9C B5 69 A6 ..i...i.
00000090 C2 97 62 A6 9F B5 69 A6 ..b...i.
00000098 E7 A9 65 A6 9E B5 69 A6 ..e...i.
000000A0 1F A9 67 A6 9A B5 69 A6 ..g...i.
000000A8 F3 AA 63 A6 97 B5 69 A6 ..e...i.
000000B0 F3 AA 6D A6 9E B5 69 A6 ..m...i.
000000B8 F3 AA 62 A6 9E B5 69 A6 ..b...i.
000000C0 CA AA 7A A6 84 B5 69 A6 ..z...i.
000000C8 9C B5 69 A6 8C B5 69 A6 ..i...i.
000000D0 FE AA 7A A6 88 B5 69 A6 ..z...i.
000000D8 C8 96 59 A6 D0 B5 69 A6 ..Y...i.
000000E0 9C B5 68 A6 29 BD 69 A6 ..h...i.
000000E8 C8 96 58 A6 09 B0 69 A6 ..X...i.
000000F0 5B B3 6F A6 9D B5 69 A6 [..o...i.
000000F8 63 95 6D A6 88 B5 69 A6 c..m...i.
00000100 52 69 63 68 9C B5 69 A6 Rich...i.
00000108 00 00 00 00 00 00 00 00 .....
00000110 00 00 00 00 00 00 00 00 .....
00000118 00 00 00 00 00 00 00 00 .....
00000120 50 45 00 00 4C 01 05 00 PE..L...
00000128 DB E7 24 3F 00 00 00 00 ..$?....
00000130 00 00 00 00 E0 00 0E 03 .....
00000138 0B 01 06 00 00 EE 4E 00 .....N.
00000140 00 BC 22 00 00 00 00 00 ..".....
```

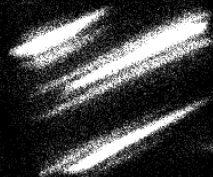
Hex / ASCII View

```
<6394910> ?IsDirectory@nsFileSpec@@QBEHXZ
<6394944> ?GetLeafName@nsFileSpec@@QBEF
<6394980> ??0nsDirectoryIterator@@QAE@ABVr
<6395030> ?Rename@nsFileSpec@@QAEIPBD@Z
<6395062> ??YnsFileSpec@@QAEIPBD@Z
<6395090> ?CopyToDir@nsFileSpec@@QBEIABV
<6395128> ?NS_NewFileSpecWithSpec@@YAIAI
<6395194> ??1nsOutputStream@@UAE@XZ
<6395226> ?close@nsOutputStream@@QAEIXZ
<6395258> ?nsEndl@@YAAVnsOutputStream@
<6395298> ??6nsOutputStream@@QAEAAV0@PI
<6395334> ?is_open@nsFileClient@@QBEHXZ
<6395366> ??0nsOutputStream@@QAE@ABV
<6395416> ?Exists@nsFileSpec@@QBEHXZ
<6395446> ??0nsDependentString@@QAE@PBG
<6395482> ??0nsFileSpec@@QAE@PBDH@Z
<6395510> ?GetCString@nsFileSpec@@QBEIPBD
<6395546> ??4nsFileSpec@@QAEABV0@Z
<6395576> ?IsFile@nsFileSpec@@QBEHXZ
<6395606> ??0nsFileSpec@@QAE@ABVnsString
<6395644> ??1nsInputStream@@UAE@XZ
<6395676> ?read@nsInputStream@@QAEHPAXI
<6395710> ??0nsInputStream@@QAE@ABVn
<6395758> ??0nsDependentCString@@QAE@PB
??_7nsAFlatCString@@6B@
<6395820> ?BeginWriting@nsASingleFragmentCSt
<6395878> ?CharAt@nsASingleFragmentCString@
<6395922> ?Delete@nsFileSpec@@QBEHXZ
<6395952> ?Error@nsFileSpec@@QBEIXZ
<6395980> ??HnsFileSpec@@QBE?AV0@PBD@
<6396012> ?flush@nsOutputStream@@UAEIX
<6396048> ?put@nsOutputStream@@QAEIXZ
<6396080> ?NS_NewFileSpecFromlFile@@YAIPA
```

Strings

# Strange Attractors and TCP/IP Sequence Number Analysis (Michal Zalewski)

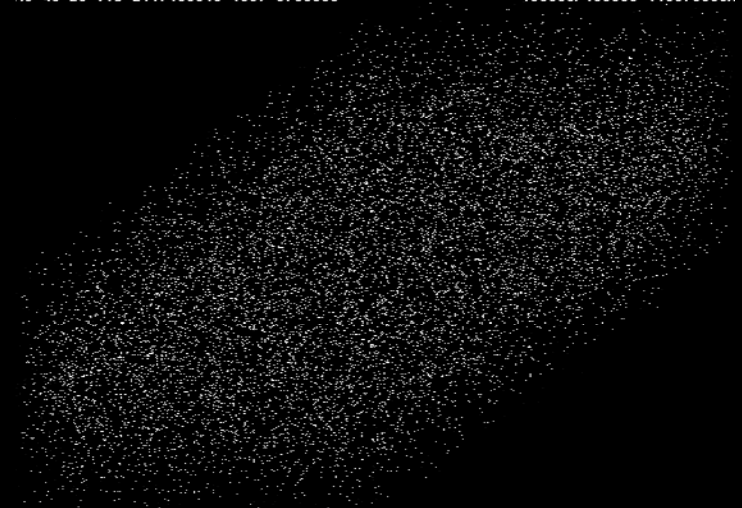
x179 y-119 28192 vis 524288 (19) 16.00000



99911/100000 (99.9110%)

08 48 28 vis 214/483648 (33) 0.00000

100000/100000 (100.0000%)



[lcamtuf] Q A O P - move, Z U - zoom/unzoom, E R - rotate

[lcamtuf] Q A O P - move, Z U - zoom/unzoom, E R - rotate

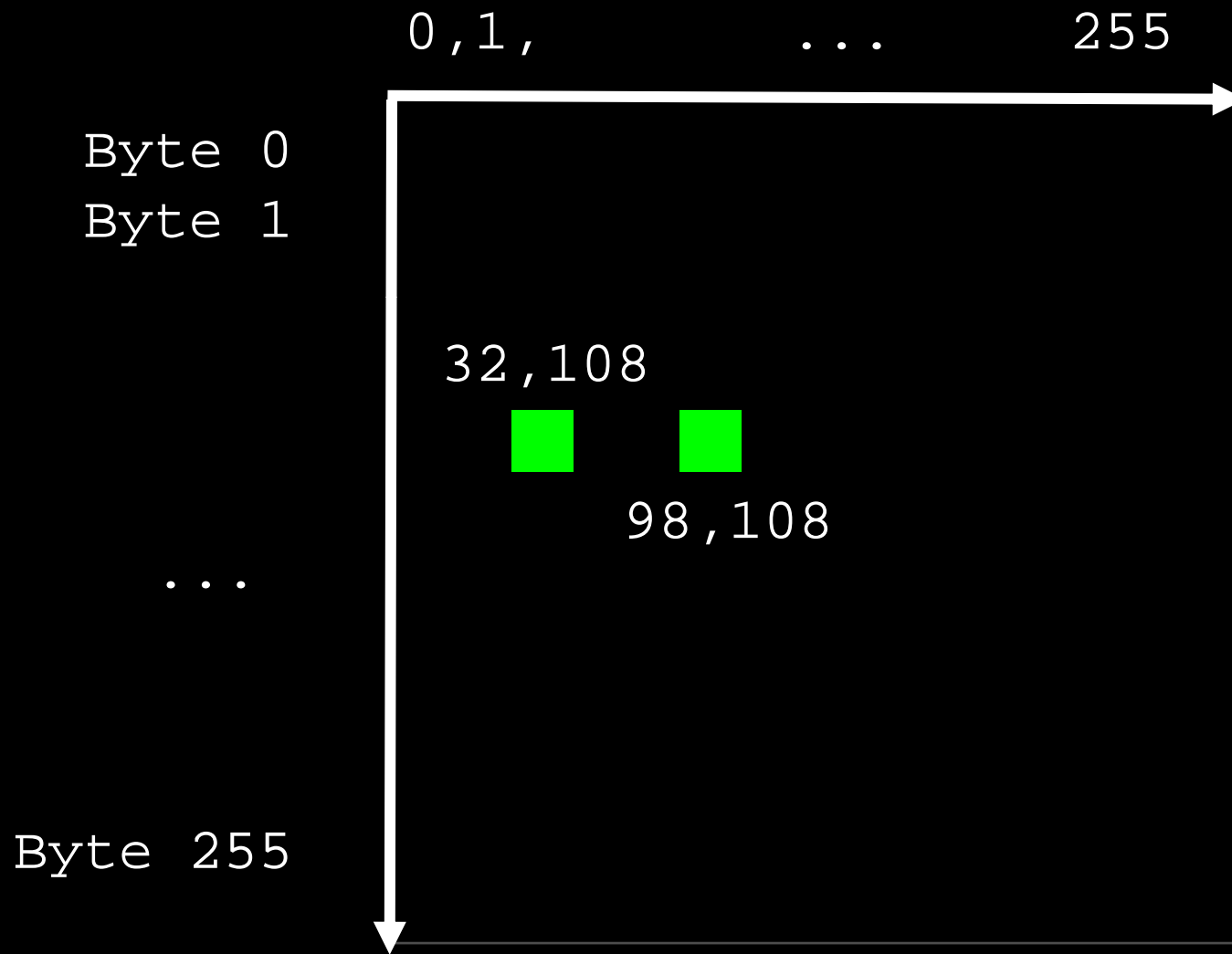
- <http://lcamtuf.coredump.cx/oldtcp/tcpseq.html>
- <http://lcamtuf.coredump.cx/newtcp/>

# Digraph View

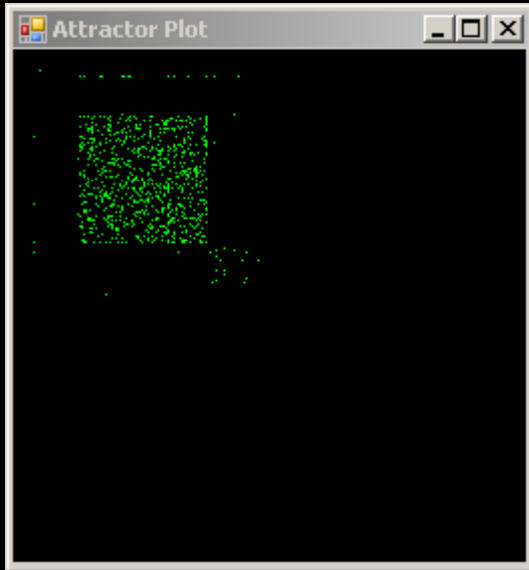
**black hat**

bl	( 98 , 108 )
la	( 108 , 97 )
ac	( 97 , 99 )
ck	( 99 , 107 )
k_	( 107 , 32 )
_h	( 32 , 104 )
ha	( 104 , 97 )
at	( 97 , 116 )

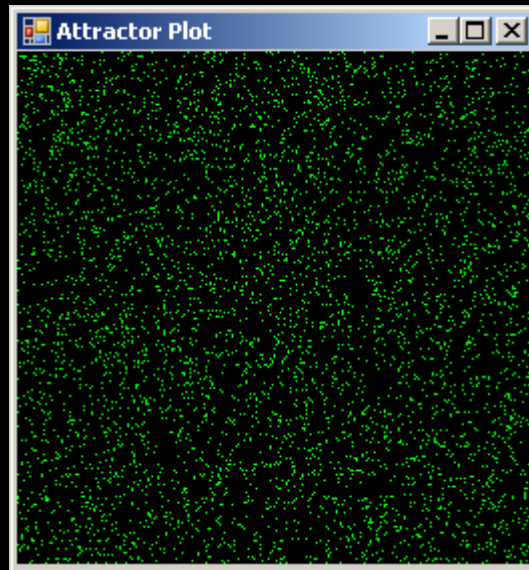
# Digraph View



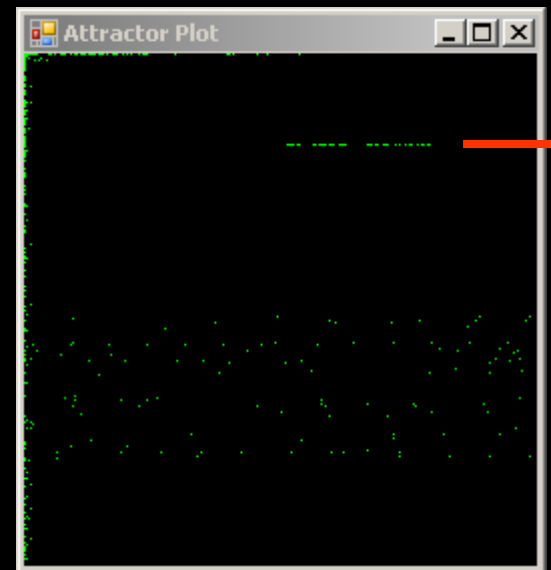




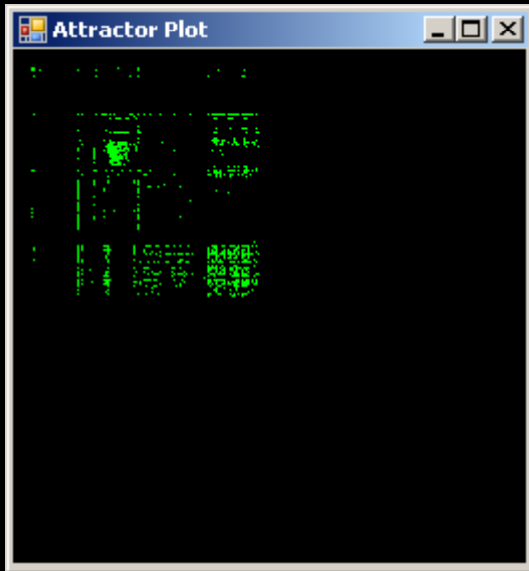
uuencoded



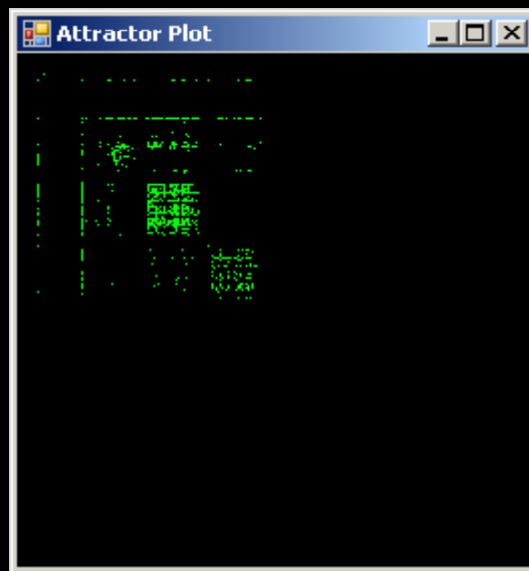
compression  
encryption



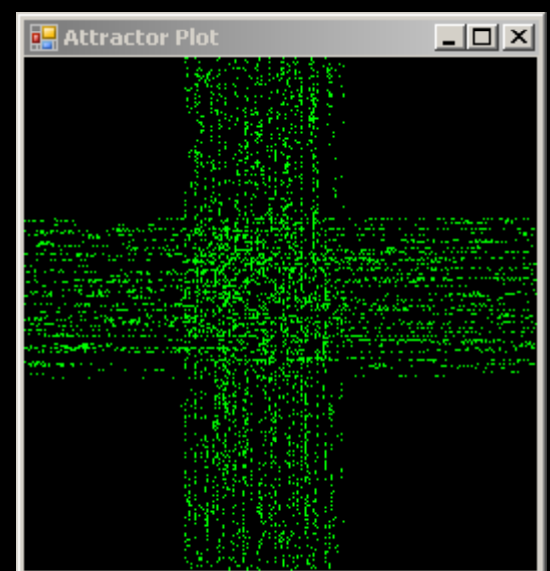
incrementing  
words



slashdot.org

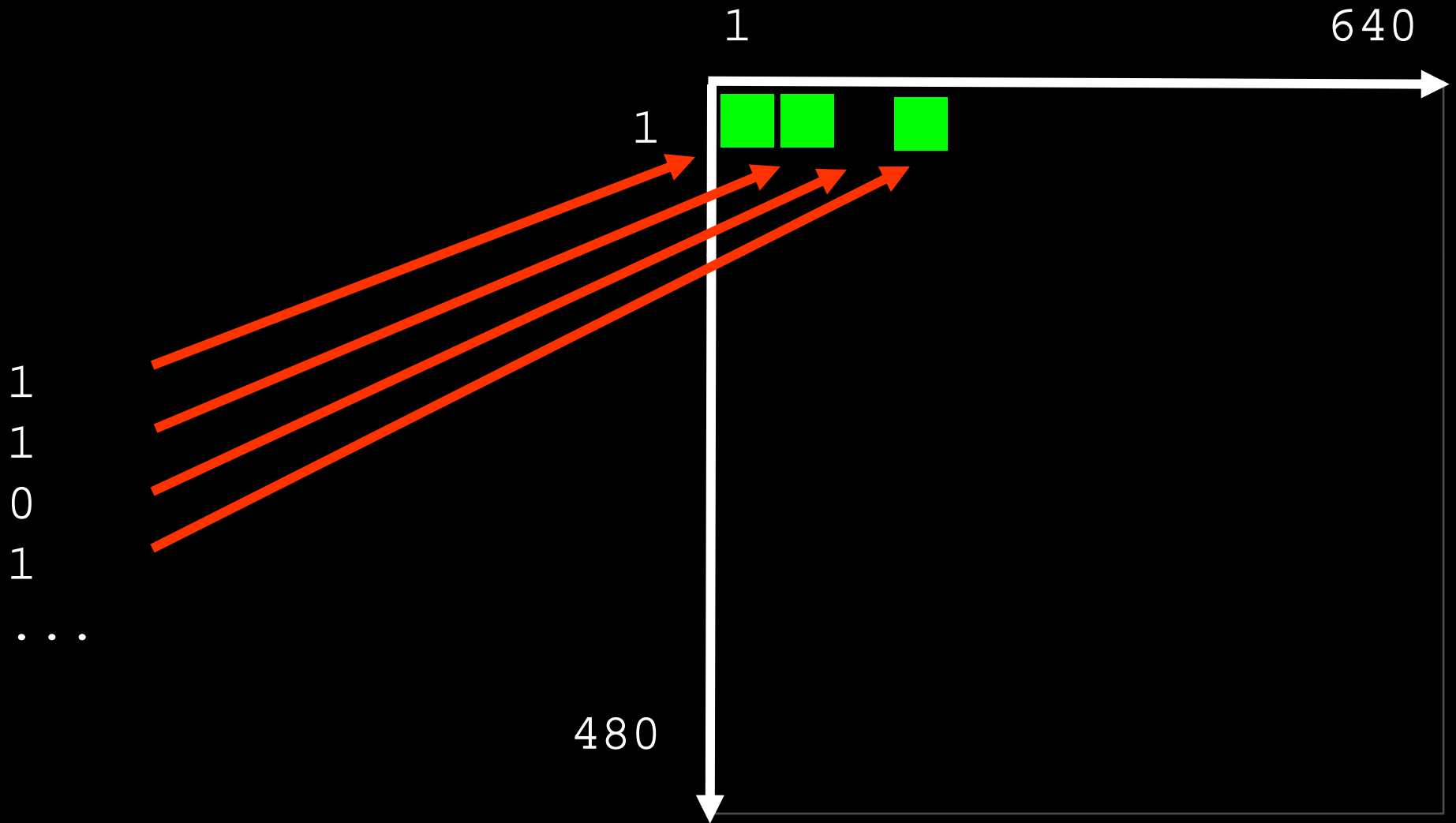


.txt

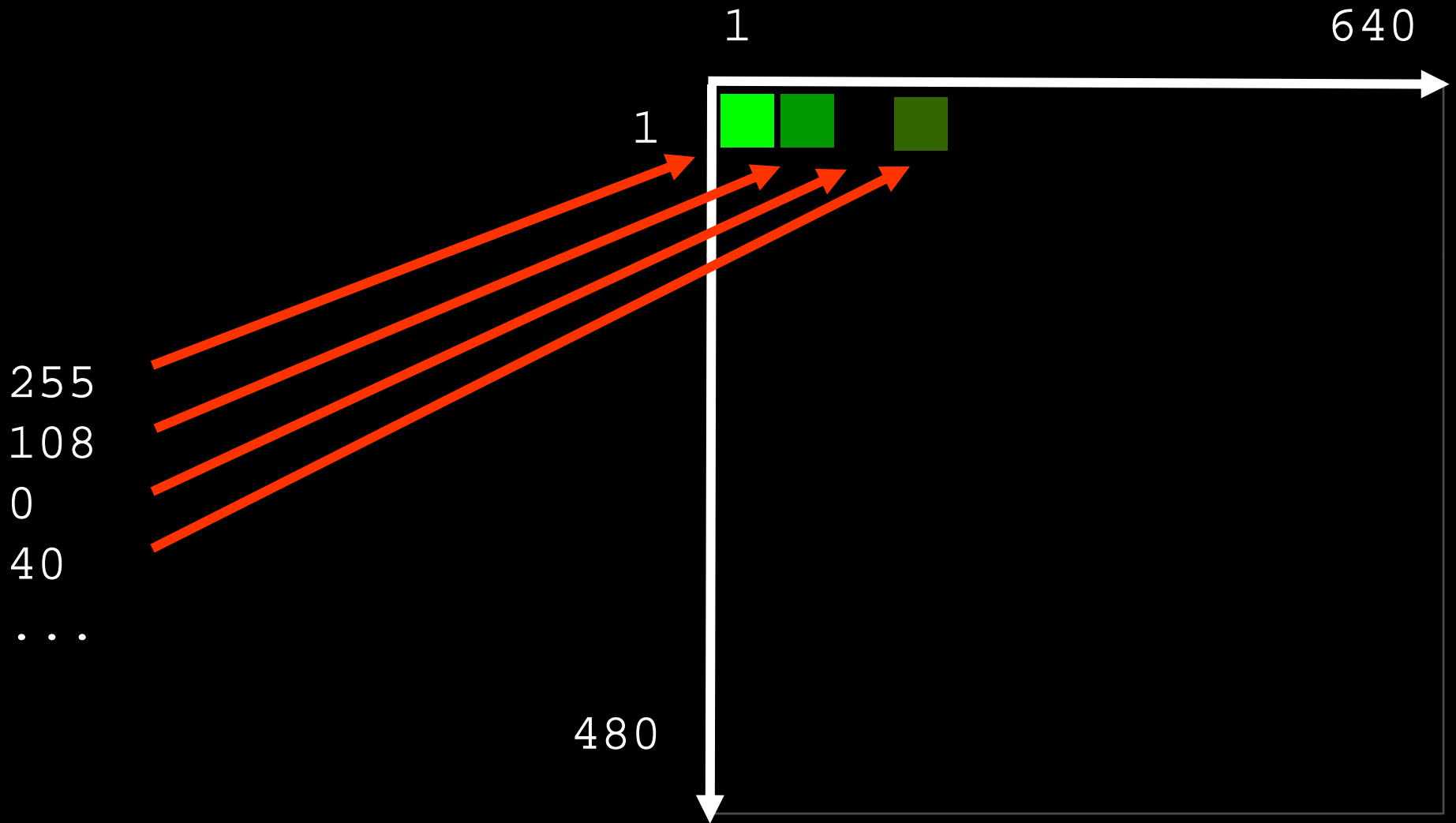


constrained pairs

# Bit Plot

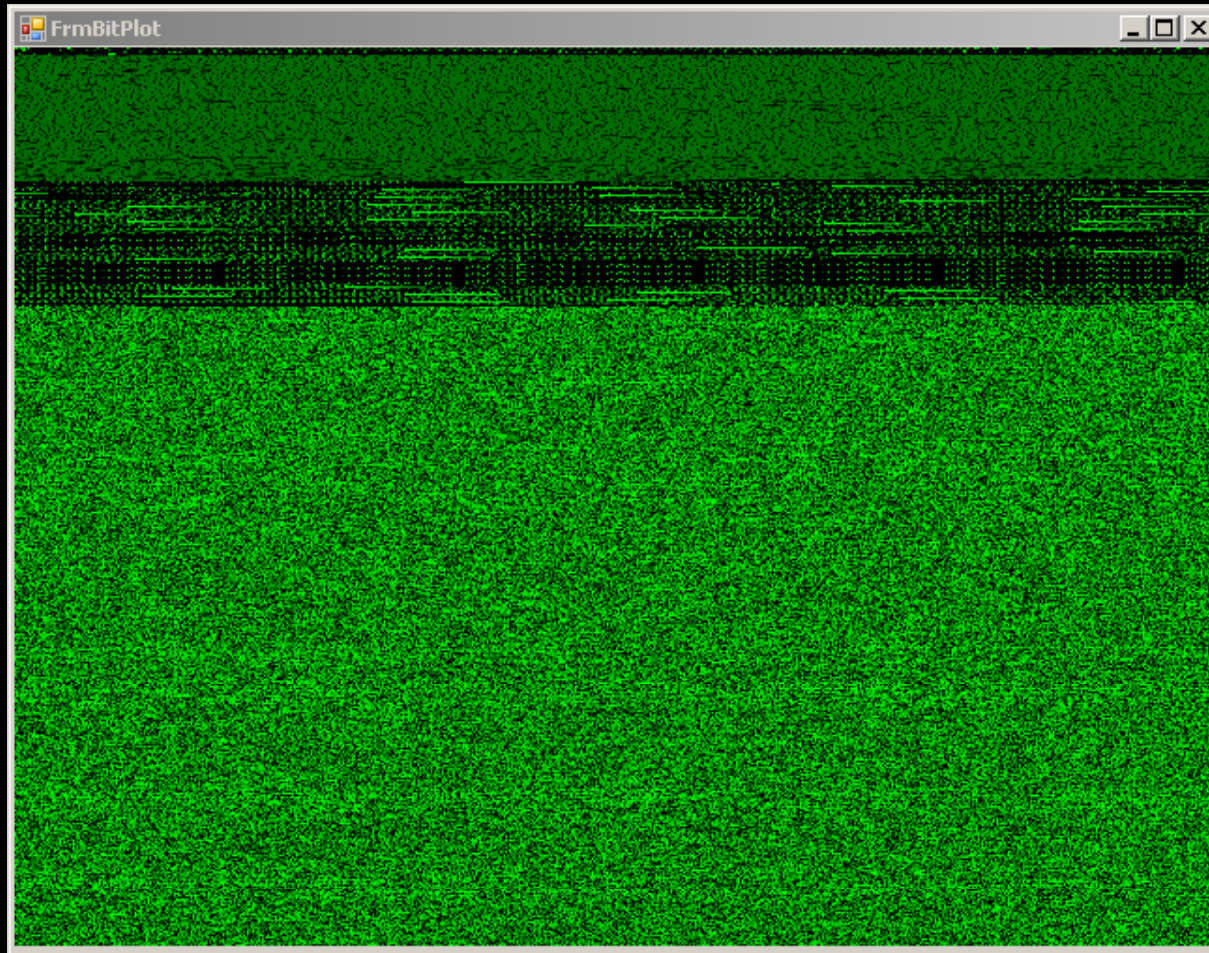


# Byte Plot

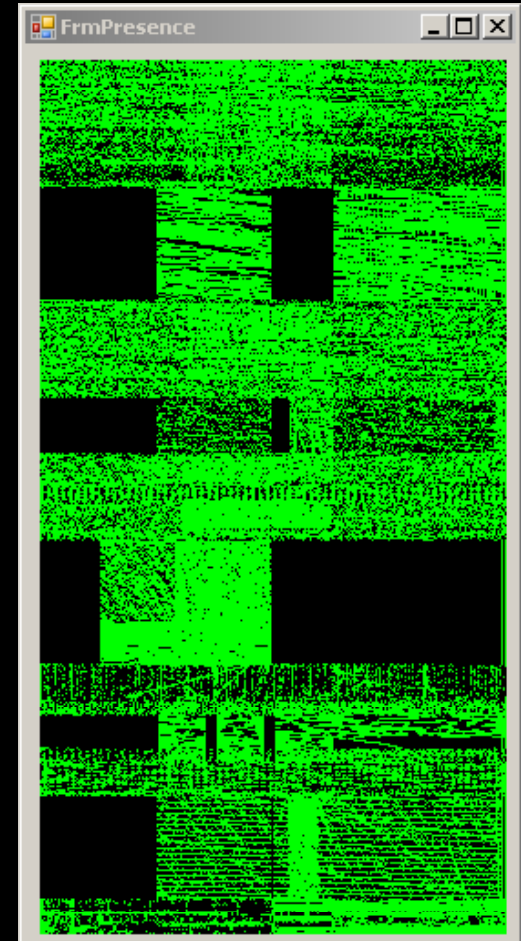
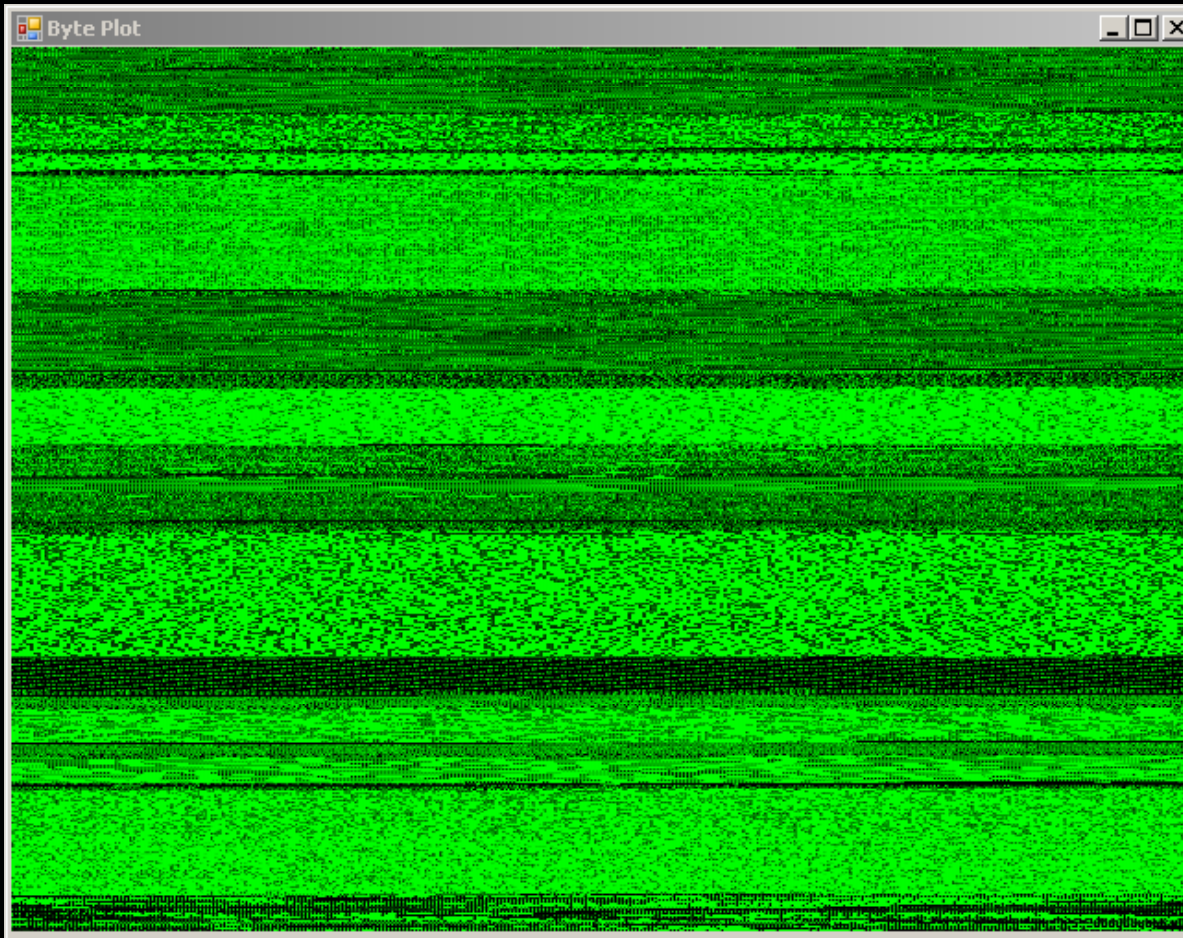


# Byte Plot Example

(Word Document)



# Byte Presence



# RGB Plot

255

108

0

1

640

40

1

128

255

0

0

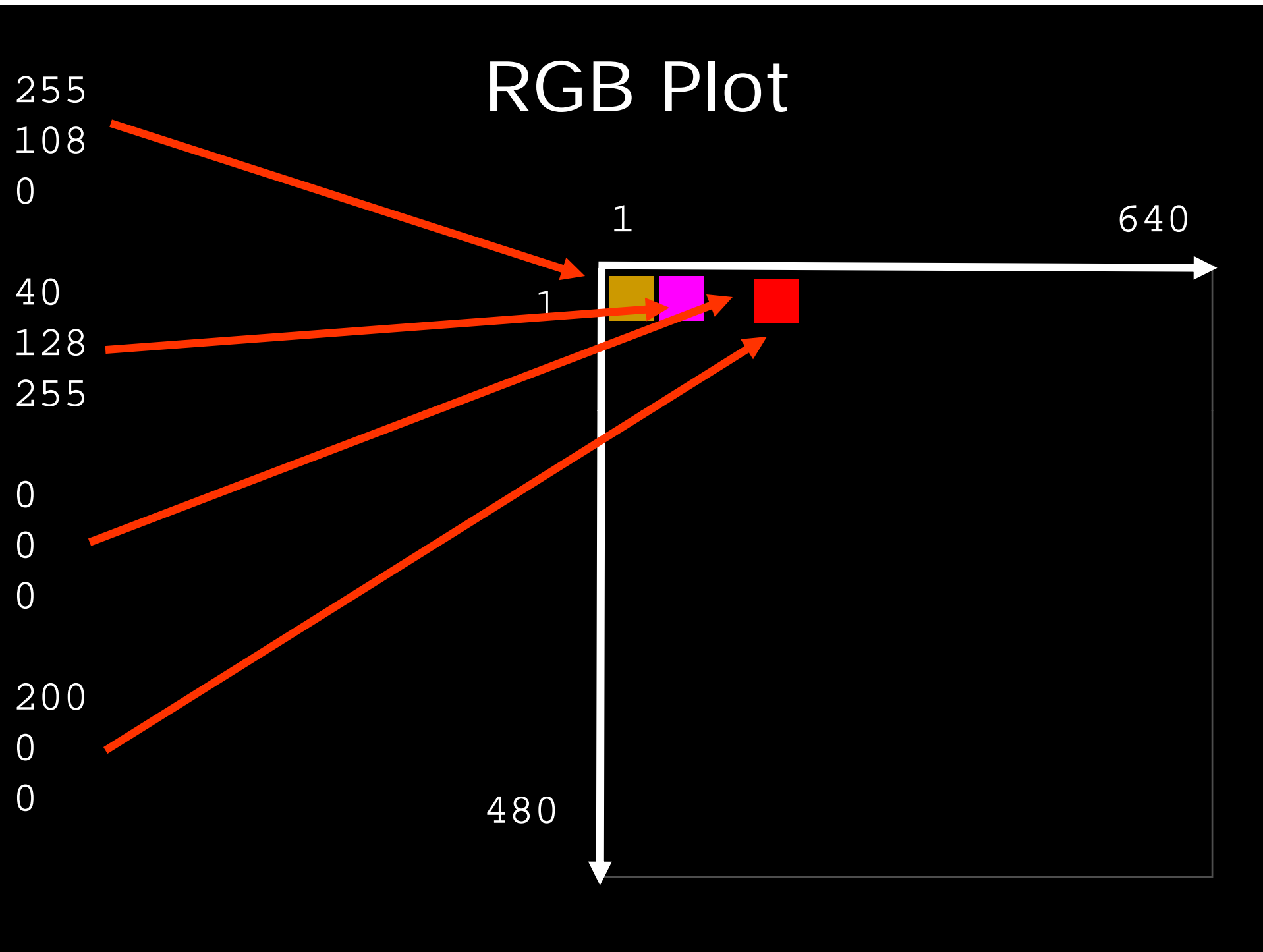
0

200

0

0

480



# Dot Plots

- Jonathan Helfman's "Dotplot Patterns: A Literal Look at Pattern Languages."
- Dan Kaminsky, CCC & BH 2006

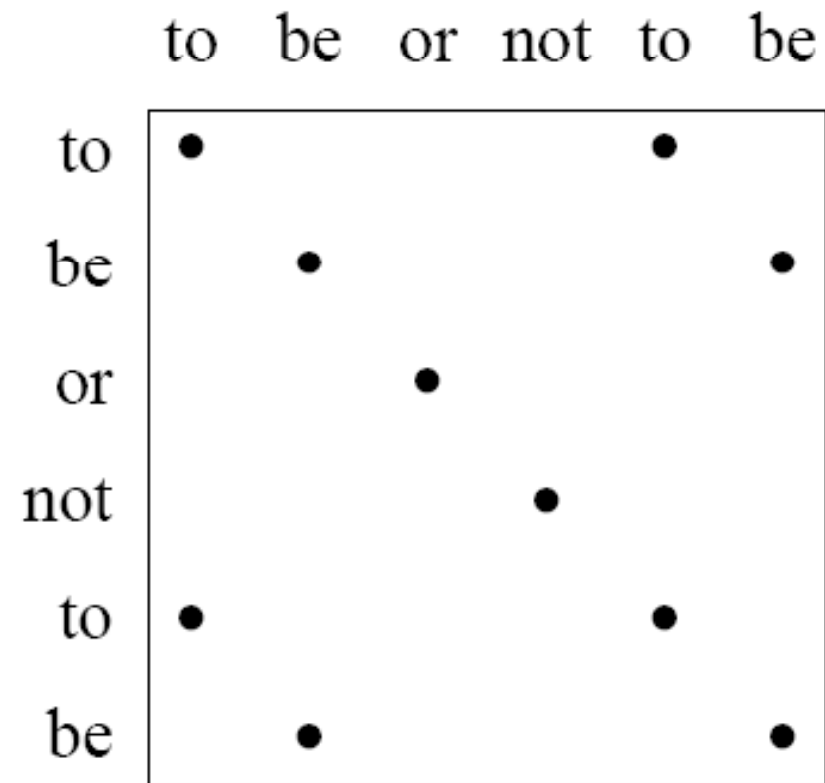
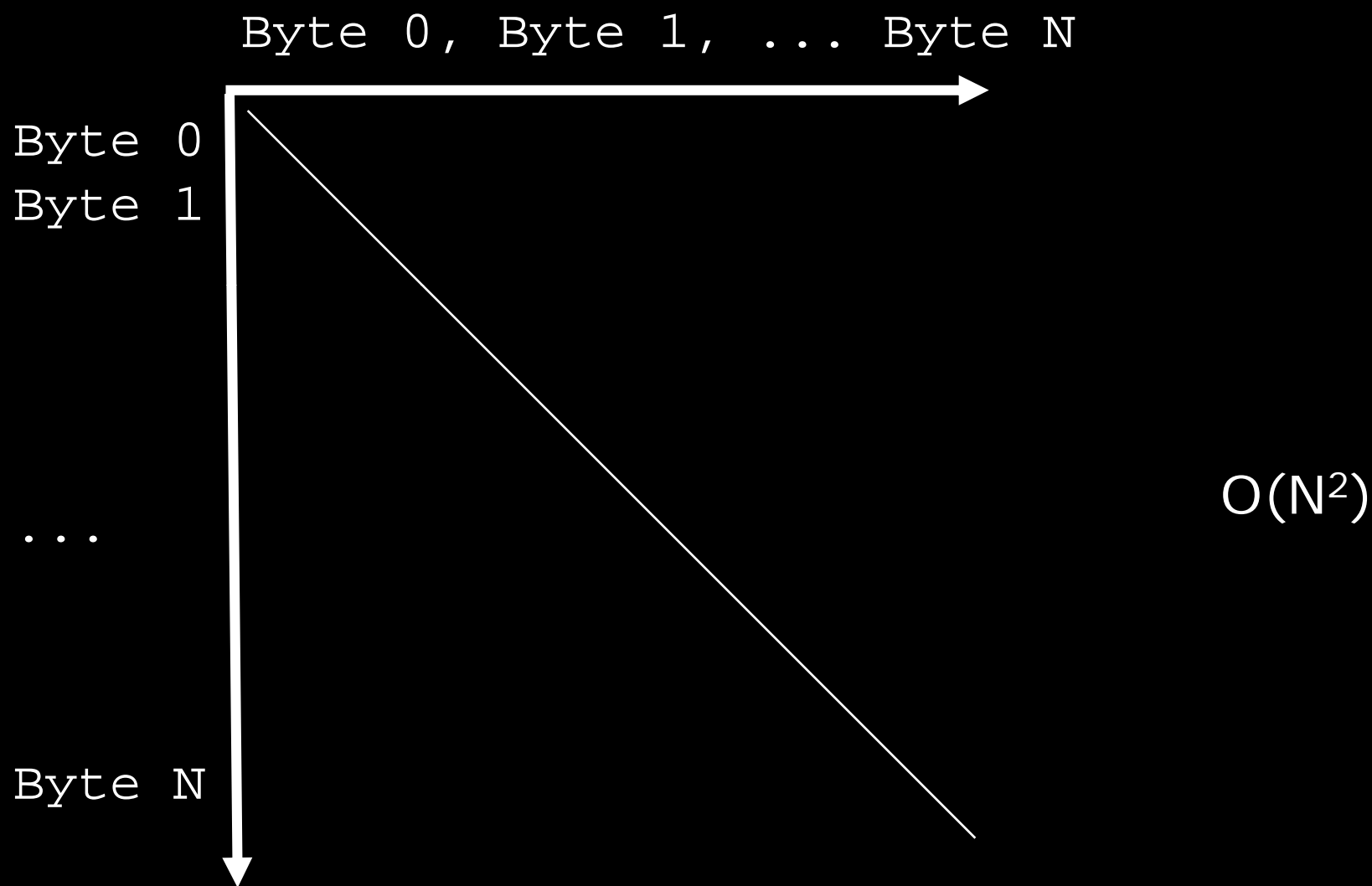


Figure 2: Six words of Shakespeare.

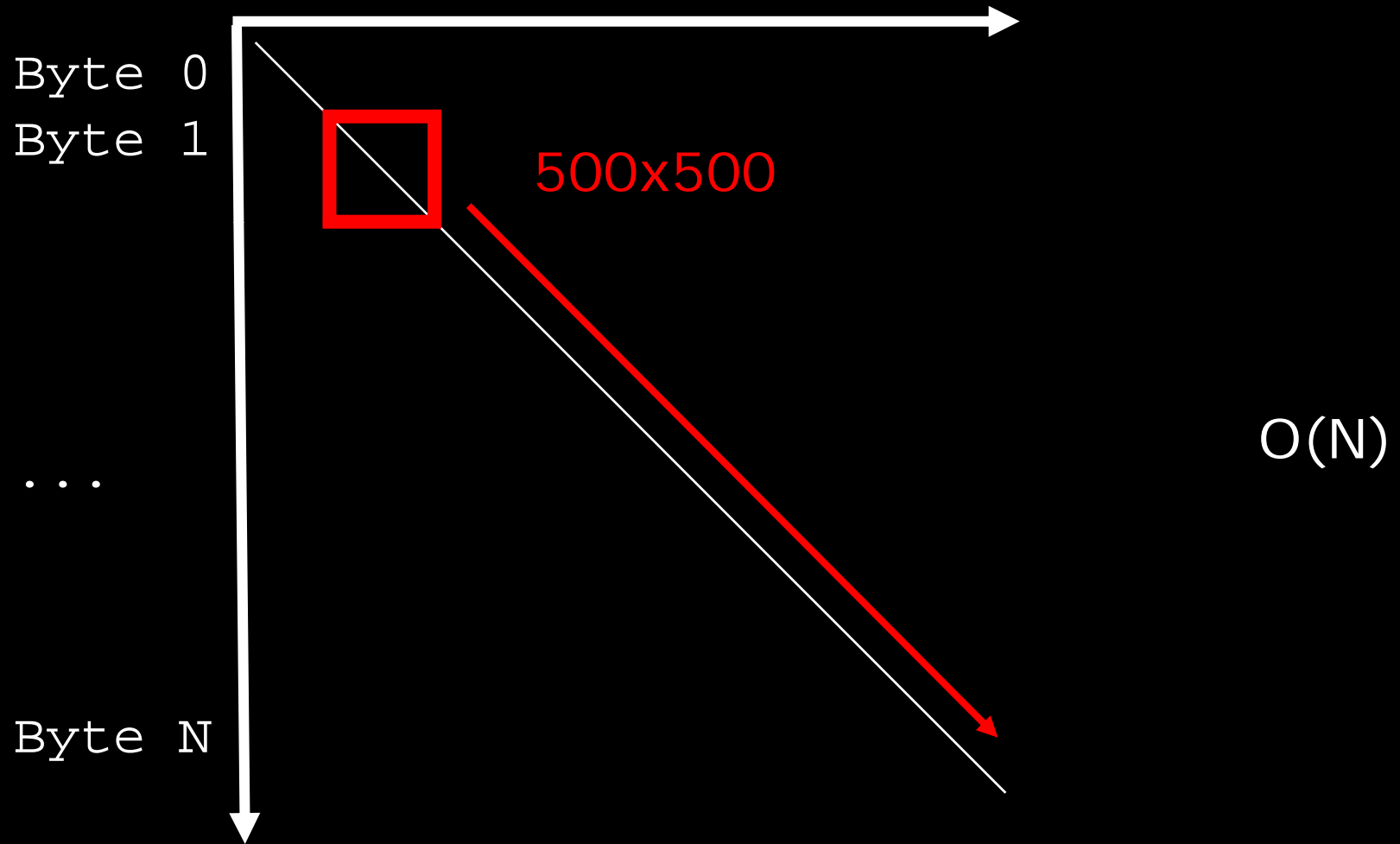
# DotPlots





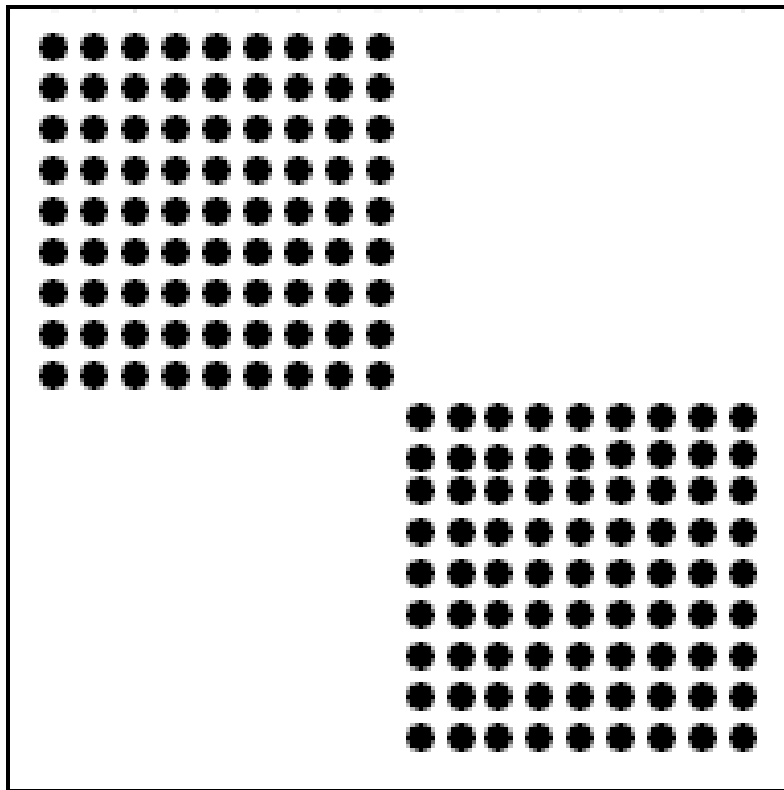
# Dynamic DotPlots

Byte 0, Byte 1, ... Byte N



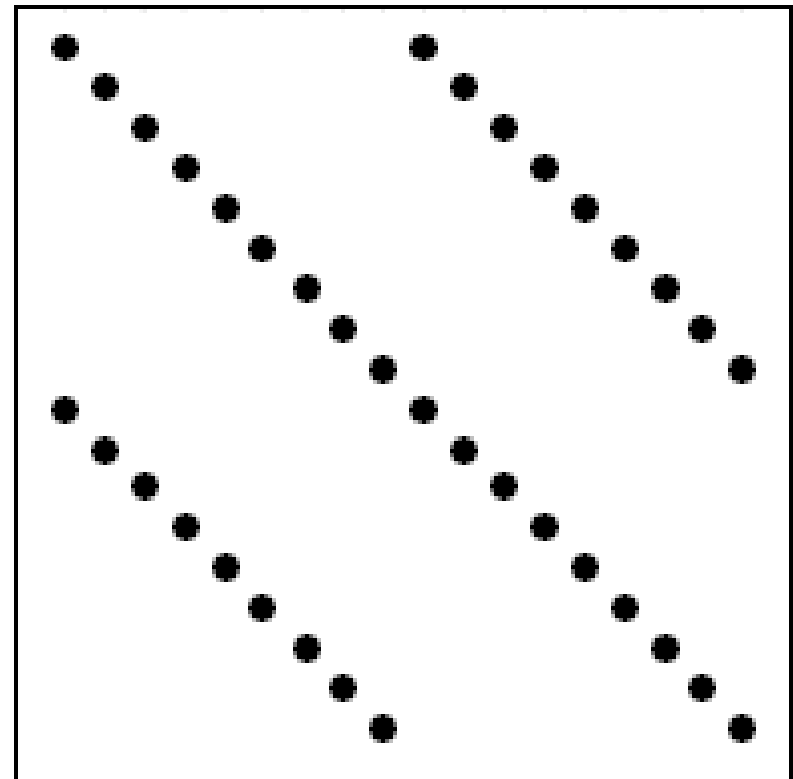
# DotPlot Examples

aaaaaaaaabbbbbbbbb



a) Squares.

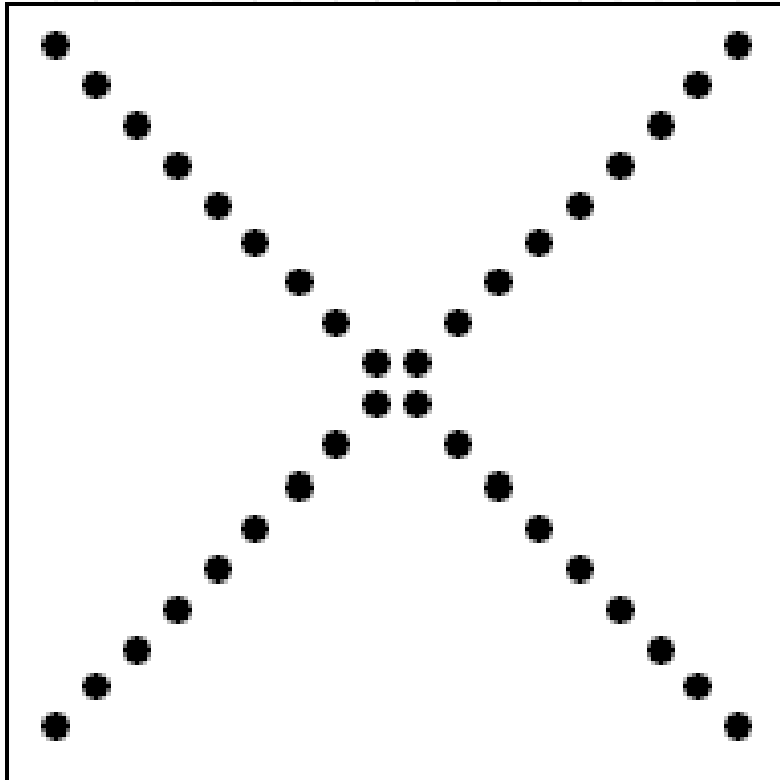
abcdefghiabcdefghi



b) Diagonals.

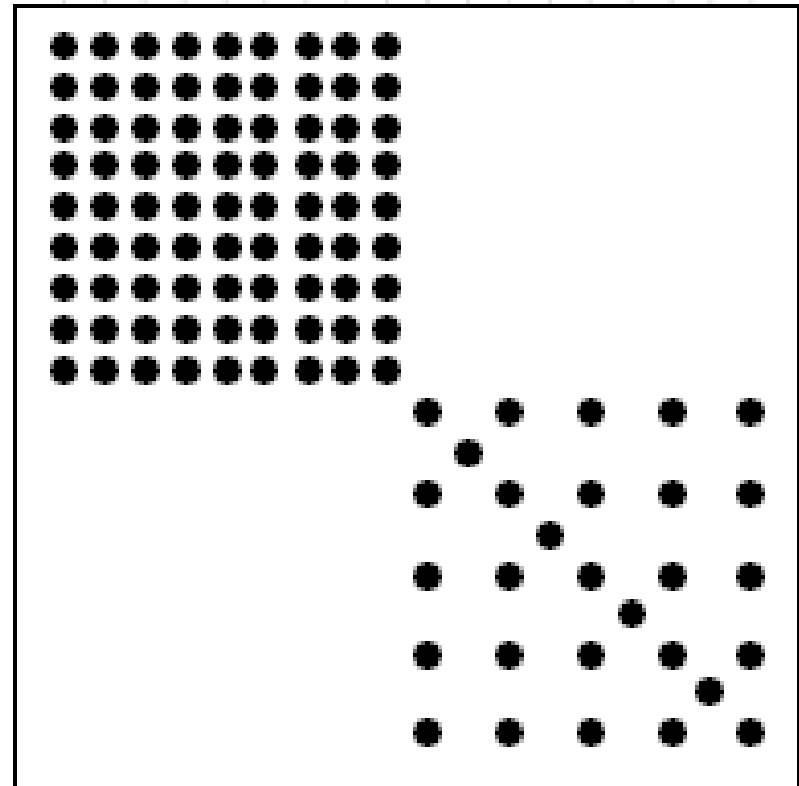
# DotPlot Examples

abcde fgh i i h g f e d c b a

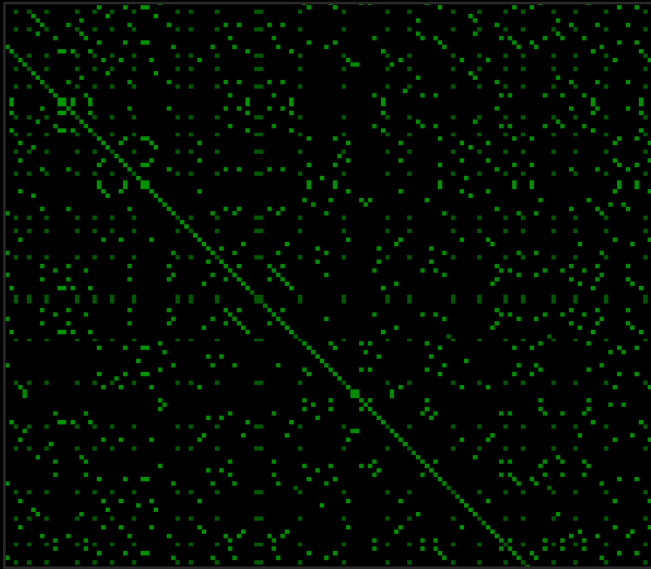


j) Palindrome.

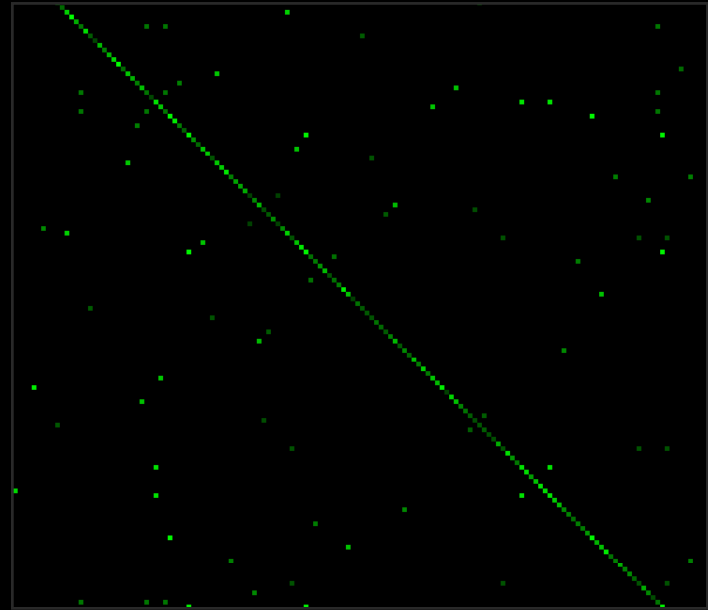
aaaaaaaaaab<sup>z</sup>b<sup>y</sup>b<sup>x</sup>b<sup>w</sup>b



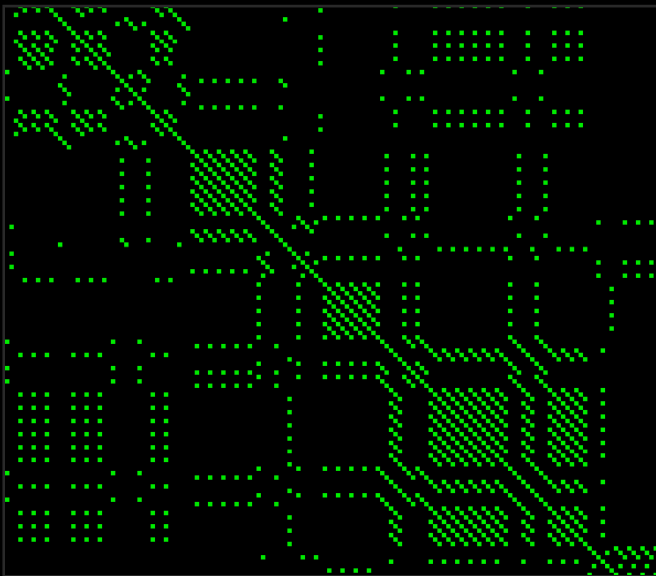
h) Density Variation.



English Text



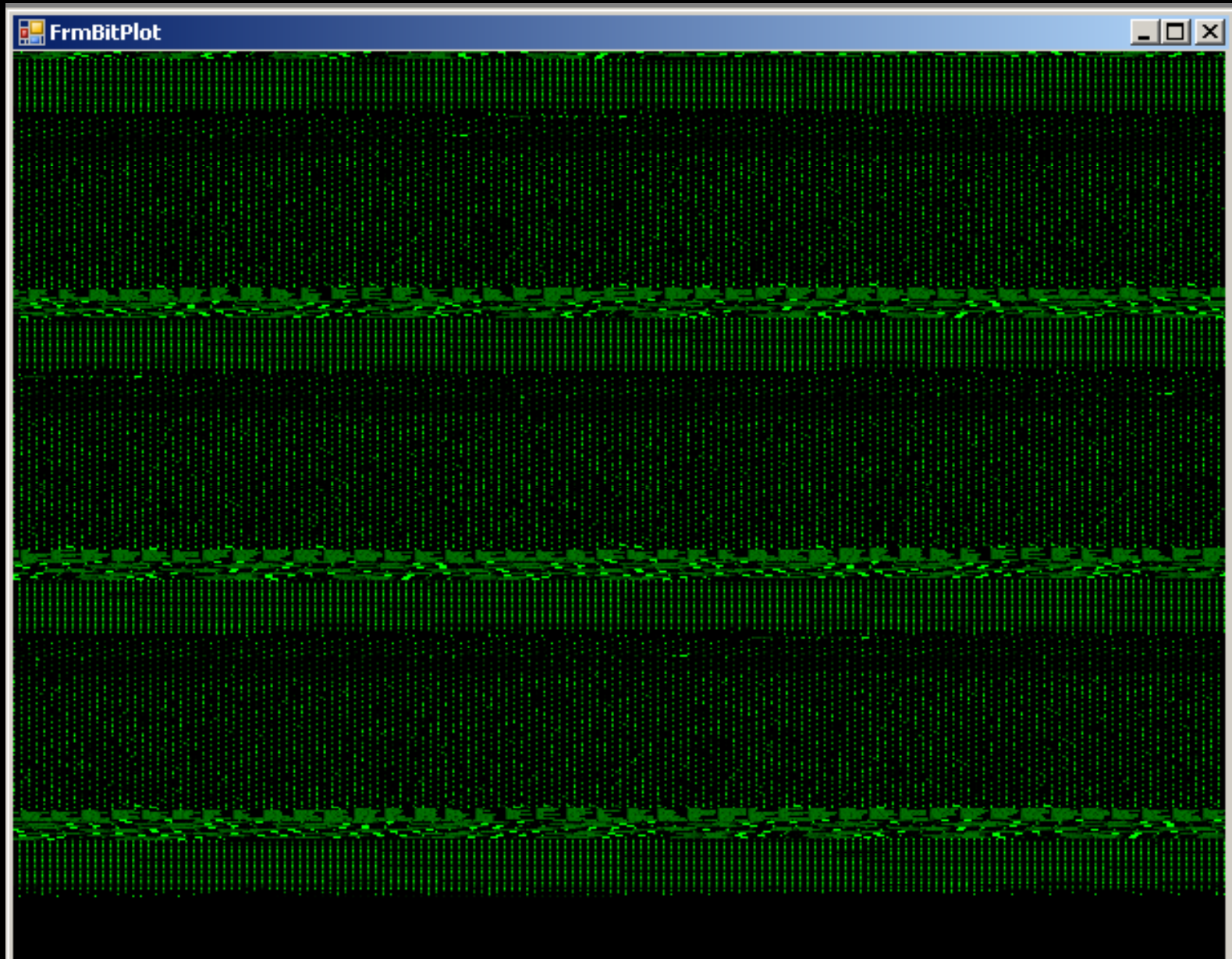
Compressed Audio

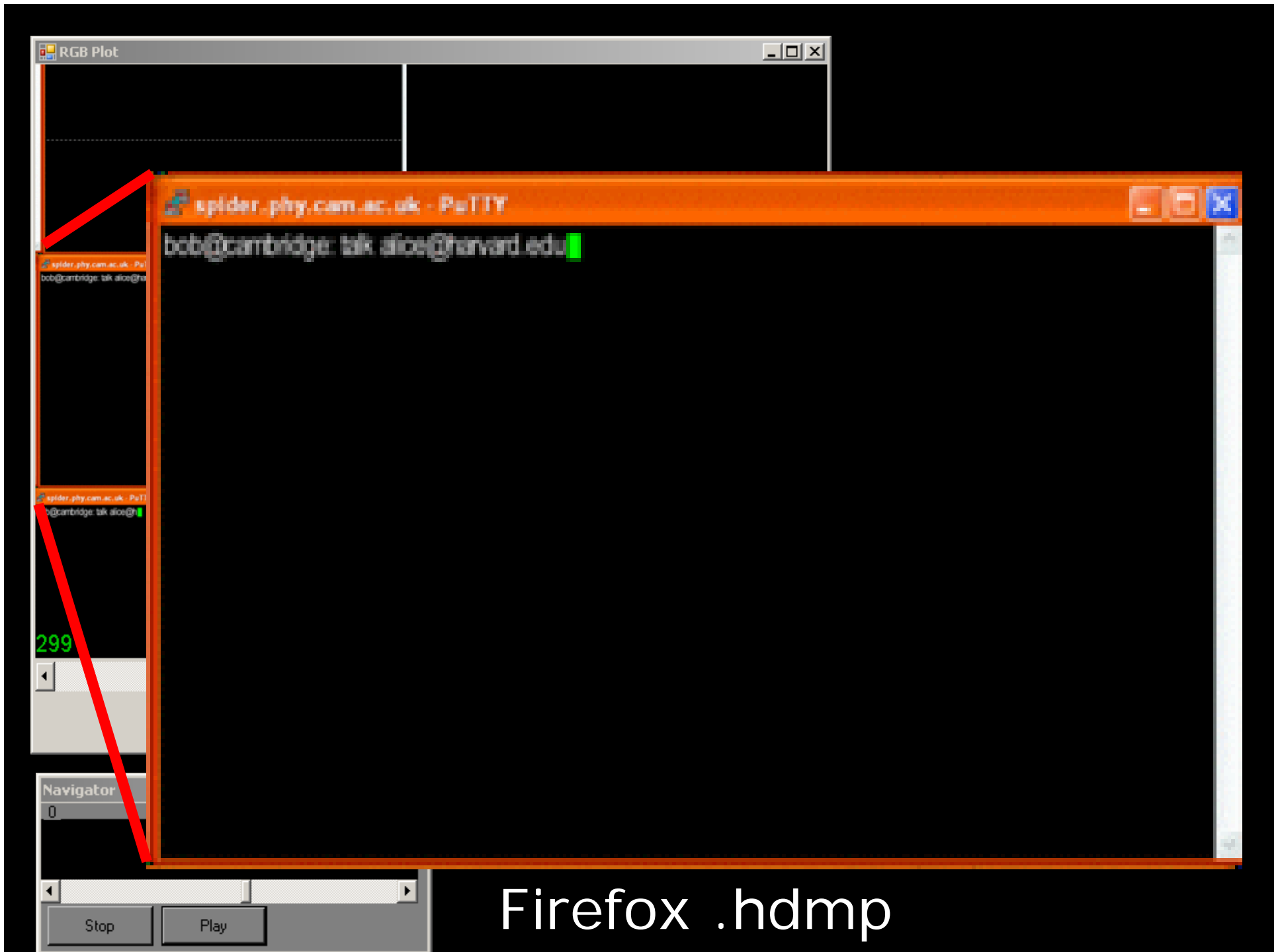


Bitmap Image

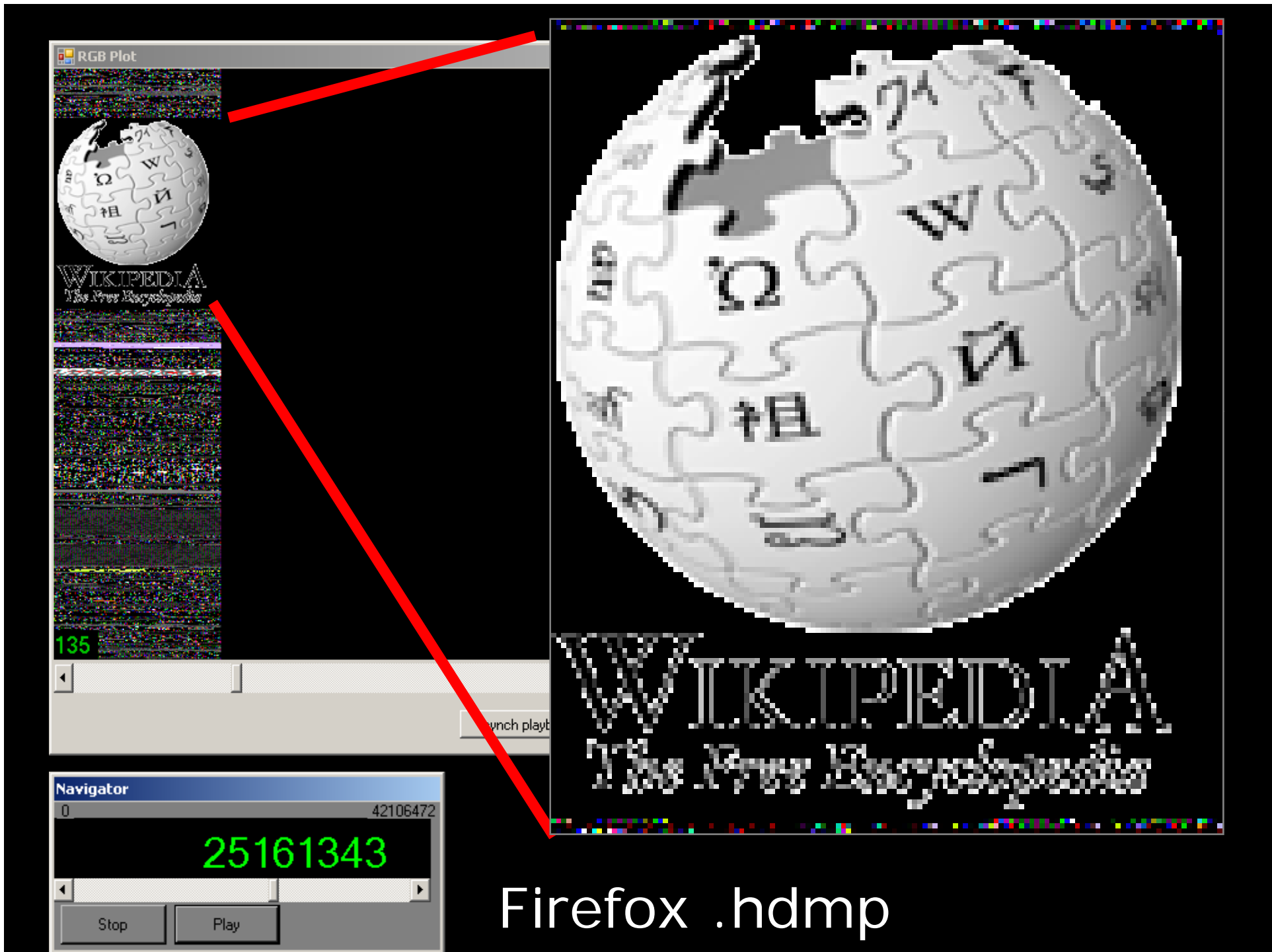


# Neverwinter Nights Database File





Firefox .hdmp

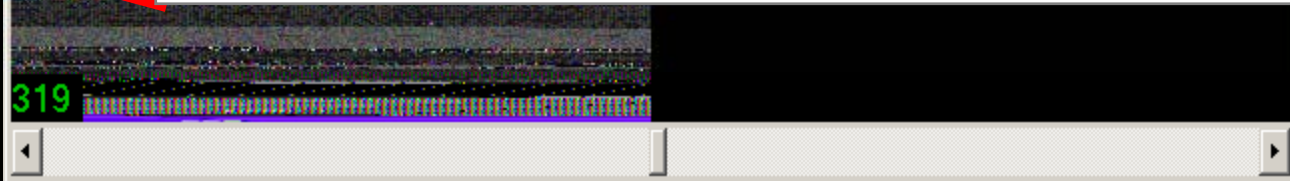
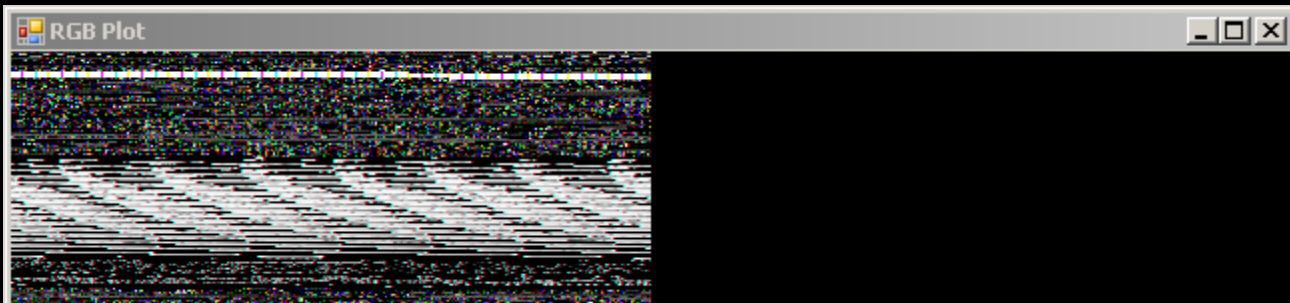


Firefox .hdmp





Firefox .hdmp



Navigator 0 42106472

24930574

Stop Play

The image shows a video player's control interface. At the top, it displays "Navigator" with a value of "0" and a total duration of "42106472". Below this, a large green number "24930574" is displayed, likely representing the current frame or a specific time value. At the bottom, there are two buttons labeled "Stop" and "Play".

synch playback to this window  flip

The image shows a control panel with a button labeled "synch playback to this window" and a checked checkbox labeled "flip".

Firefox .hdmp

BinVis C:\Documents and Settings\rumint\Desktop\fbireport\_igcaleafinal.pdf

File View

Navigator  
0 309036  
**16364**  
Stop Play

Byte Plot

Attractor Plot

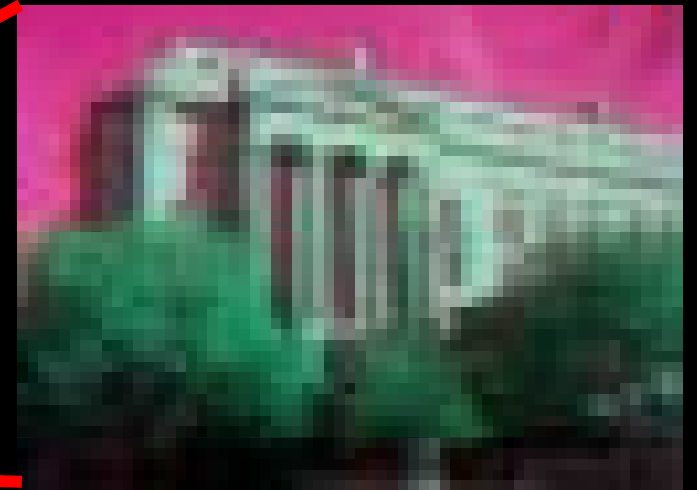
Text

```
00045609 30 30 30 30 30 30 00000000
00045611 30 20 36 35 35 33 20 0 65535
00045613 66 0d 0a 30 30 30 30 f..00000
00045621 30 30 30 30 20 36 35 00000 65
00045629 35 33 35 20 66 0d 0a 30 535 f..0
00045631 30 30 30 30 30 30 00000000
00045639 30 20 36 35 35 33 20 0 65535
00045641 66 0d 0a 30 30 30 30 f..00000
00045649 30 30 30 30 20 36 35 00000 65
00045651 35 33 35 20 66 0d 0a 30 535 f..0
00045659 30 30 30 30 30 30 00000000
00045661 30 20 36 35 35 33 20 0 65535
00045669 66 0d 0a 30 30 30 30 f..00000
00045671 30 30 30 30 20 36 35 00000 65
00045679 35 33 35 20 66 0d 0a 30 535 f..0
00045681 30 30 30 30 30 30 00000000
00045689 30 20 36 35 35 33 20 0 65535
00045691 66 0d 0a 30 30 30 30 f..00000
00045699 30 30 30 30 20 36 35 00000 65
000456A1 35 33 35 20 66 0d 0a 30 535 f..0
000456A9 30 30 30 30 30 30 00000000
000456B1 30 20 36 35 35 33 20 0 65535
000456B9 66 0d 0a 30 30 30 30 f..00000
000456C1 30 30 30 30 20 36 35 00000 65
000456C9 35 33 35 20 66 0d 0a 30 535 f..0
000456D1 30 30 30 30 30 30 00000000
000456D9 30 20 36 35 35 33 20 0 65535
000456E1 66 0d 0a 30 30 30 30 f..00000
000456E9 30 30 30 30 20 36 35 00000 65
000456F1 35 33 35 20 66 0d 0a 30 535 f..0
000456F9 30 30 30 30 30 30 00000000
00045701 30 20 36 35 35 33 20 0 65535
00045709 66 0d 0a 30 30 30 30 f..00000
00045711 30 30 30 30 20 36 35 00000 65
00045719 35 33 35 20 66 0d 0a 30 535 f..0
00045721 30 30 30 30 30 30 00000000
00045729 30 20 36 35 35 33 20 0 65535
00045731 66 0d 0a 30 30 30 30 f..00000
00045739 30 30 30 30 20 36 35 00000 65
00045741 35 33 35 20 66 0d 0a 30 535 f..0
00045749 30 30 30 30 30 30 00000000
```

RGB Plot

63

synch playback to this window  flip



Redacted  
PDF...

# Weaknesses

- entire file may be extracted from bit/byte/RGB
  - May trigger AV or IDS
  - 8bit/byte steg
- Screams for big monitor

# Demos

# A Look to the Future...

- Visual Front Ends for Offensive Tools
- Visual Cryptanalysis Support
- Human Insights Passed to Machine Processors
- User-centric Evaluation
- More Inspiration from General InfoVis Community
- Visual Fingerprints / Smart Books
- Web-based Visualization (AJAX)
- User-task Analyses
  - True Use Case Based Designs
  - Engagement of Users Beyond Students
- Examination of Full Range of Security Data
  - Merging Multiple Security Dataflows

# Future Work

- Plug-ins / Editable Config Files
  - Visualizations
  - Encodings
- Saving state
  - Memory Maps
- Improving Interaction
  - What works / What doesn't
- Multiple Files / File Systems
- REGEX search
- Automated Memory Map Generation

# DAVIX

(Jan Monsch and Raffy Marty)

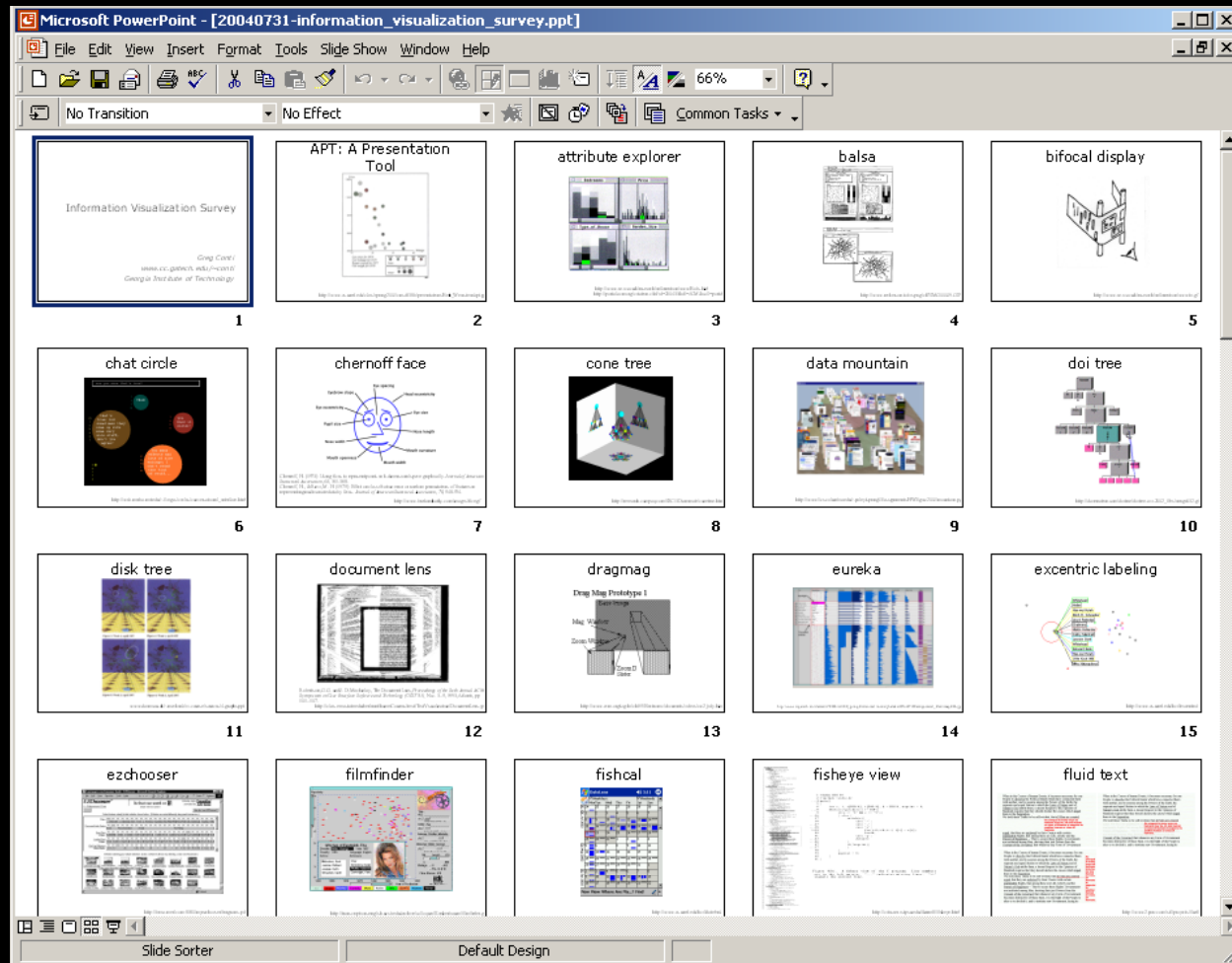
The screenshot displays a KDE 3.5 desktop environment. The desktop background is a gradient of orange and yellow. The top-left corner features the DAVIX Homepage icon. A menu is open, showing a list of applications including Afterglow, ChartDirector, Cytoscape, EtherApe, Gobi, gITail, GNUplot, Graphviz, GUESS, InetVis, Large Graph Layout (LGL), Mondrian, MRTG, NvisionIP, Parvis, Ploticus, Project, RRTool, RT Graph 3D, rumint, Scapy, Shoki, Timesearcher 1, tny, Treemap, Tulip, and Walrus. The taskbar at the bottom shows several open windows: InetVis Display, EtherApe, and eth0: Capturing - Wireshark. The InetVis Display window shows a 3D network graph with nodes and edges. The EtherApe window shows a network graph with nodes and edges, and a list of protocols including WWW, ICMP, UDP-Unkn, TCP, POP3s, NETBIOS, and SMB. The eth0: Capturing - Wireshark window shows a packet capture table with columns for No., Time, Source, Destination, Protocol, and Info.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.16.220	255.255.255.255	UDP	Source port: 56472
2	0.001961	192.168.16.220	192.168.16.1	DNS	Standard query PTR
3	0.024332	192.168.16.1	192.168.16.220	DNS	Standard query res
4	0.253749	192.168.16.220	255.255.255.255	ICMP	Echo (ping) request
5	0.01177	00:0c:29:2c:b0:6f	00:00:24:c5:69:8c	ARP	Who has 192.168.16.1
6	0.02832	00:00:24:c5:69:8c	00:0c:29:2c:b0:6f	ARP	192.168.16.1 is at
7	17.366520	192.168.16.140	80.239.228.18	TCP	1433 > 80 [FIN, ACK]
8	17.378497	192.168.16.220	192.168.16.1	DNS	Standard query PTR
9	17.407005	80.239.228.18	192.168.16.140	TCP	80 > 1433 [FIN, ACK]
10	17.407040	192.168.16.140	80.239.228.18	TCP	1433 > 80 [ACK] Seq
11	17.841488	192.168.16.1	192.168.16.220	DNS	Standard query request
12	01.073472	192.168.16.220	192.168.16.1	DNS	Standard query response
13	01.216347	192.168.16.1	192.168.16.220	DNS	Standard query response

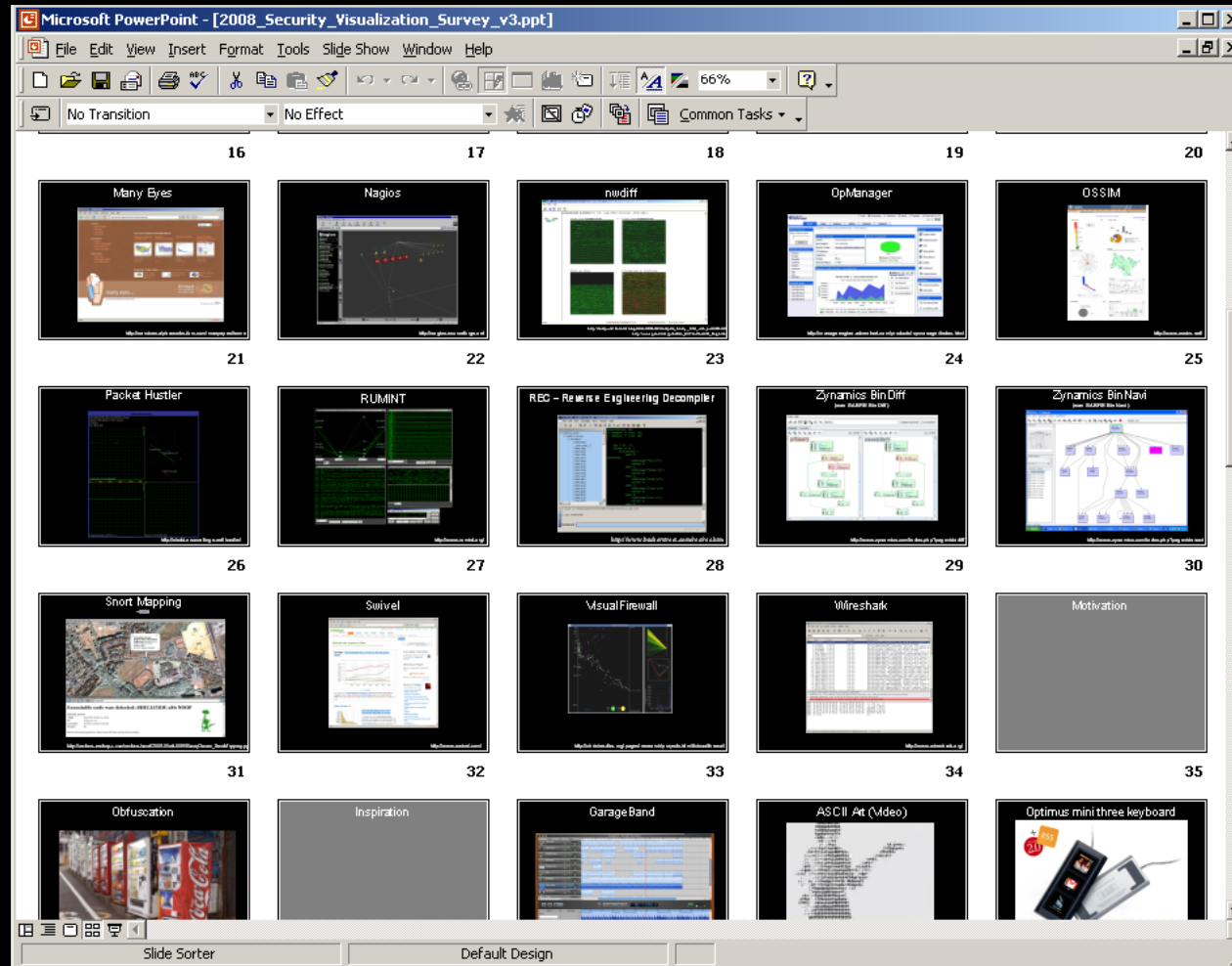
<http://www.secviz.org/node/89>



# InfoVis Survey



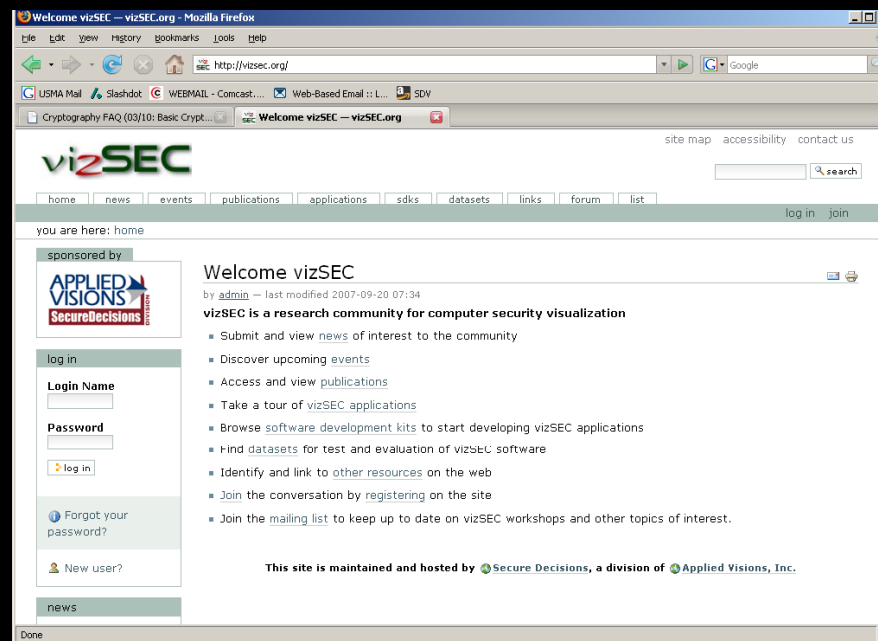
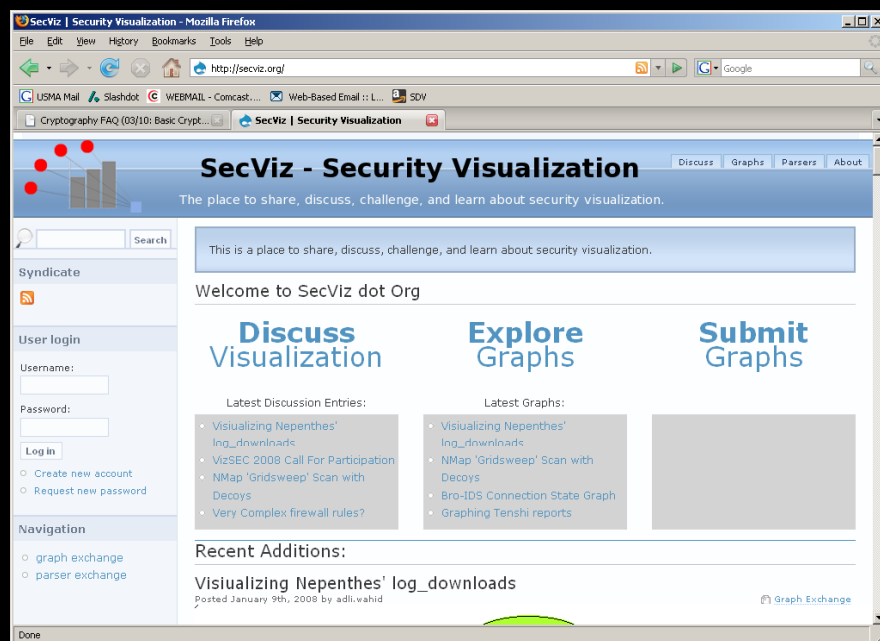
# Security Visualization Survey



# Communities

<http://secviz.org/>

<http://vizsec.org/>



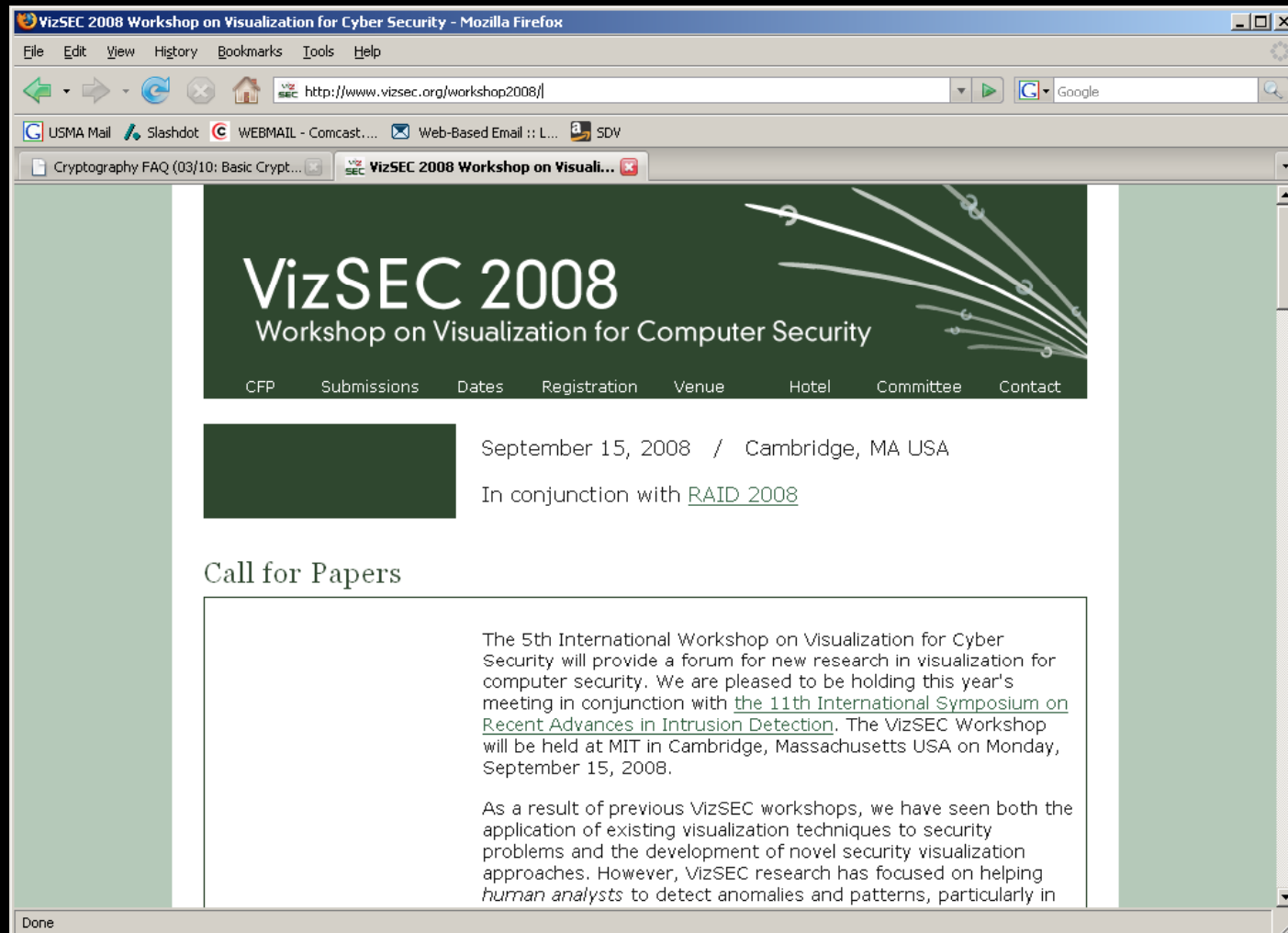
“The place to share, discuss, challenge, and learn about security visualization.”

Raffy Marty  
Splunk

“vizSEC is a research community for computer security visualization.”

John Goodall  
Secure Decisions

# VizSEC 2008



The screenshot shows a Mozilla Firefox browser window displaying the website for the VizSEC 2008 Workshop on Visualization for Computer Security. The browser's address bar shows the URL <http://www.vizsec.org/workshop2008/>. The website features a dark green header with the text "VizSEC 2008 Workshop on Visualization for Computer Security" and a navigation menu with links for CFP, Submissions, Dates, Registration, Venue, Hotel, Committee, and Contact. Below the header, the dates "September 15, 2008 / Cambridge, MA USA" and the text "In conjunction with [RAID 2008](#)" are displayed. A section titled "Call for Papers" contains the following text:

The 5th International Workshop on Visualization for Cyber Security will provide a forum for new research in visualization for computer security. We are pleased to be holding this year's meeting in conjunction with [the 11th International Symposium on Recent Advances in Intrusion Detection](#). The VizSEC Workshop will be held at MIT in Cambridge, Massachusetts USA on Monday, September 15, 2008.

As a result of previous VizSEC workshops, we have seen both the application of existing visualization techniques to security problems and the development of novel security visualization approaches. However, VizSEC research has focused on helping *human analysts* to detect anomalies and patterns, particularly in

<http://www.vizsec.org/workshop2008/>

# More Information

- “Visual Reverse Engineering of Binary and Data Files.” Gregory Conti, Erik Dean, Matthew Sinda, Benjamin Sangster. VizSEC 2008.
  - Available September
- Security Data Visualization (No Starch Press)
- Applied Security Visualization (Addison-Wesley)

## Visual Reverse Engine

Gregory Conti, Erik Dean

Department of Electric  
United S

We

{gregory.conti, erik.dean, ma

### Abstract.

The analysis of computer files pe seeking to detect and analyze malicio formats for their products, and fo behavior and structure of undocumen editors, disassemblers and debuggers text based approaches. In this pape which support meaningful investigat

# Acknowledgements

Damon Becknell, Jon Bentley, Jean Blair, Sergey Bratus, Chris Compton, Tom Cross, Ron Dodge, Carrie Gates, Chris Gates, Joe Grand, Julian Grizzard, Toby Kohlenberg, Oleg Kolesnikov, Frank Mabry, Raffy Marty, Brent Nolan, Gene Ressler, Ben Sangster, Matt Sinda, and Ed Sobiesk

"In fact, master reversers like Fravia recommend cracking while intoxicated with a mixture of strong alcoholic beverages.

While for health reasons we cannot recommend this method, you may find that a relaxing cup of hot tea unwinds your mind and allows you to think in reverse."

-from *Security Warrior*