





# Agenda

- . Overview of Data Forensics
- . Agents of Change
- . Future of Data Forensics
- . Linux as Next Generation Data Forensics platform
- . Questions



# Data Forensics, Infancy

Historically data forensics has focused on imaging and analyzing standalone personal computers (PCs).

- small hard drives
- DOS-based utilities



# Evolving Data Forensics

First agents of change;

- significantly larger hard drives (>500MB)
- significant increase in number of PCs
- increase in use of PCs in crimes



# Evolving Data Forensics

Second agents of change;

- significant increase in use of non-PC devices
  - servers, handhelds, digital cameras, etc.
- increase in non-Windows operating systems
  - MacOS, UNIX flavors, Linux flavors, etc.



# Evolving Data Forensics

Where does the data forensic community stand today?

Electronic data is stored in many devices, ranging from wrist watches, telephony boxes, and enterprise servers. Increasingly forensic examiners are dealing with 'non-traditional' PCs, corporate security personnel are first responders to incidents, and critical data is residing in volatile system memory.



# NG Forensics Defined

"The scientific process of imaging and analyzing data stored in any electronic format, for the purpose of reporting findings in a neutral manner, with no predisposition as to guilt or innocence."

farmerdude,

2002



# NG Forensics & Linux

Next generation data forensics platform of choice?

**Linux**





# NG Forensics & Linux

What makes Linux so powerful?

- everything, including hardware, is a file
- support for numerous file system types
- ability to analyze a live system in a minimally invasive manner
- ability to chain commands
- ability to monitor and log processes & commands
- ability to review source code
- ability to create bootable media



# NG Forensics & Linux

File Recognition within Linux;

- ease of replication (clear text config files)
- seeing everything as a file allows for a degree of control over that file
  - degree of security
  - degree of granularity over how the operating system environment behaves



# NG Forensics & Linux

File Recognition within Linux;

- So what is the benefit to the forensic examiner?

- examiner has ability to control how the operating system touches devices

- (I.E., consistent mounting of devices in a read only manner that does not alter the data on the evidentiary device)



# NG Forensics & Linux

Numerous File System Types Support;

- Linux can interpret many file system types, including; ext2, ext3, FFS, HPFS, FAT, VFAT, NTFS, ISO9660, UDF, UFS, etc.
- Win32 can interpret a few file system types, including; FAT, VFAT, and NTFS



# NG Forensics & Linux

Numerous File System Types Support;

- So what does this mean for the examiner?
  - If you use Win32 as your platform for analysis and you wish to view data in its logical format, then you must have a driver for that specific file system type written.
  - Win32 + no fs driver = one big blob



# NG Forensics & Linux

Numerous File System Types Support;

- So what does this mean for the examiner?
  - If you use Linux as your platform for analysis and you wish to view data in its logical format, chances are you already have a driver for that fs type available for use
  - Linux + fs driver = pretty logical format



# NG Forensics & Linux

Analyzing a Live System, Minimally Invasively;

- Almost all compromised systems have trojaned commands
- Linux provides a method for analyzing this compromised system, in its running state, in a minimally invasive manner



# NG Forensics & Linux

Analyzing a Live System, Minimally Invasively;

- The goal of all data forensic work is to not alter the evidence wherever possible
- Extremely difficult to perform
- However, Linux can prove helpful





# NG Forensics & Linux

Analyzing a Live System, Minimally Invasively;

- Trusted binaries on trusted media (floppy, CD)
- Use Vi editor to issue commands without stepping all over the system logs
- Commands such as 'script' can be used in conjunction with 'time' to provide an accurate log of what commands were issued and at what time



# NG Forensics & Linux

## Chaining Commands;

- commands useful to the forensic examiner may be chained together in order to increase productivity

- example;

```
dd if=/dev/hdd conv=noerror bs=1024 of=image1 2>>  
image_error_log ; md5sum image1 > image1_hash
```



# NG Forensics & Linux

## Chaining Commands;

- Linux also provides ability to redirect standard input/output/error

- examples;

```
dd if=/dev/sda conv=noerror bs=1024 | gzip > scsi_image.gz
```

```
dd if=/dev/sda conv=noerror bs=1024 | split -b 640m
```

```
cat xa* > new_sda_image_file
```



# NG Forensics & Linux

Ability to Monitor and Log Processes & Commands;

- Linux provides an environment rich in auditing and logging user activities
- Value to forensic examiner? Trail of what happened when and by whom or what.
- Commands include; script, w, pstree, ps, strace, lsof, etc.



# NG Forensics & Linux

Source Code Review;

- most all commands used by a forensic examiner on the Linux platform are open source, and therefore, their code is freely available for review
- allows for customization of code
- more importantly, allows for increased technical knowledge (knowing what's happening 'behind the scenes') and



# NG Forensics & Linux

Trusted Boot Media;

- Whether a floppy diskette or a CD-ROM, bootable Linux media can be created and customized
- Allows forensic examiner to create personalized toolsets for most any situation, as well as trusted binaries to use for processing



# NG Forensics & Linux

What does all of this mean?

- The power of Linux empowers the forensic examiner



# NG Forensics & Linux

Questions?