Anti-Forensics:
Techniques, Detection and Countermeasures

Simson L. Garfinkel
Naval Postgraduate School

What is Anti-Forensics?

Computer Forensics: *"Scientific Knowledge for collecting, analyzing, and presenting evidence to the courts" (USCERT 2005)*

Anti-Forensics: *tools and techniques that frustrate forensic tools, investigations and investigators*

Goals of Anti-Forensics:

- *Avoiding detection*
- *Disrupting information collection*
- *Increasing the examiner's time*
- *Casting doubt on a forensic report or testimony (Liu and Brown, 2006)*

- *Forcing a tool to reveal its presence*
- *Subverting the tool — using it to attack the examiner or organization*
- *Leaving no evidence that the AF tool has been run*

One traditional Anti-Forensic technique is to overwrite or otherwise destroy data.

Overwriting: Eliminate data or metadata (e.g. disk sanitizers, Microsoft Word metadata “washers,” timestamp eliminators.)

Disk Sanitizers; Free Space Sanitizers; File Shredders

- Microsoft **Remove Hidden Data Tool**; **cipher.exe; ccleaner**

Metadata Erasers

- Example: **timestomp**

Hard problem: *What should be overwritten?*

Anti-Forensic tools can hide data with cryptography or steganography.

- Cryptographic File Systems (EFS, TrueCrypt)
- Encrypted Network Protocols (SSL, SSH, Onion Routing*)
- Program Packers (PECompact, Burneye) & Rootkits
- Steganography
- Data Hiding in File System Structures
  - Slacker — Hides data in slack space
  - FragFS — Hides in NTFS Master File Table
  - RuneFS — Stores data in “bad blocks”
  - KY FS — Stores data in directories
  - Data Mule FS — Stores in inode reserved space
  - Host Protected Areas & Device Configuration Overlay

*Onion routing also protects from traffic analysis

Anti-Forensics 3: Minimizing the Footprint

Overwriting and Data Hiding are *easy to detect.*

- Tools leave tell-tale signs; examiners know what to look for.
- Statistical properties are different after data is overwritten or hidden.

AF tools that minimize footprint avoiding leaving traces for later analysis.

- Memory injection and syscall proxying
- Live CDs, Bootable USB Tokens
- Virtual Machines
- Anonymous Identities and Storage

(don't worry; we have slides for each of these)

Memory Injection and Userland Execve: Running a program without loading the code.

Memory Injection loads code without having the code on the disk.

- **Buffer overflow** exploits — run code supplied as (oversized) input

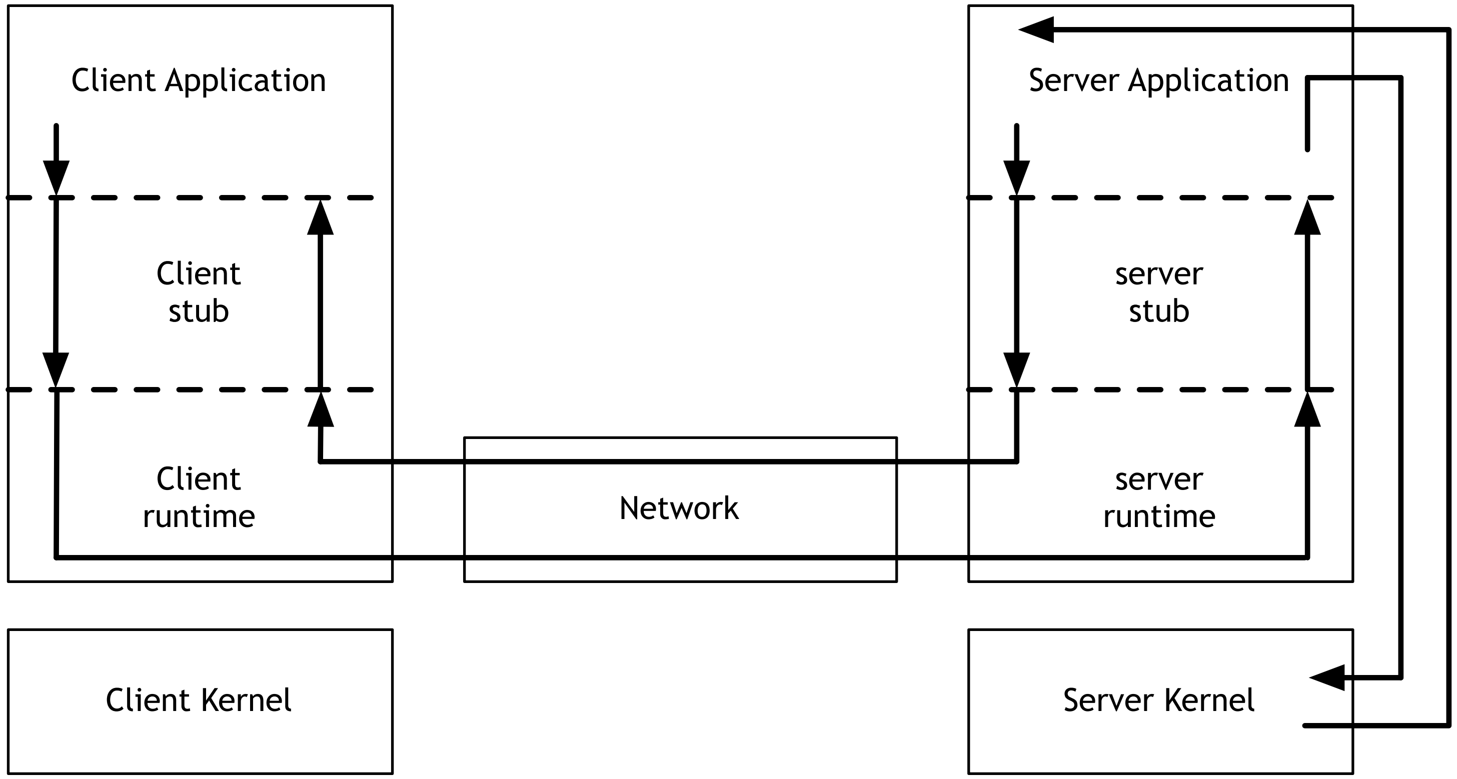
Userland Execve

— Runs program without using execve()
— Bypasses logging and access control
— Works with code from disk or read from network

Syscall proxying:
Running a program without the code!

Syscall Proxying

- Program runs on one computer, syscalls executed on another.
- Program not available for analysis
- May generate a lot of network traffic
- Developed by Core Security; used in **Impact**



Live CDs, Bootable USB Tokens, Virtual Machines: Running code without leaving a trace.

Most forensic information is left in the file system of the running computer.

These approaches keep the attacker's file system segregated:
— In RAM (CDs & Bootable USB Tokens)
— In the Virtual Machine file (where it can be securely deleted)

Anonymous Identities and Storage: The attacker’s data may be anywhere.

Attackers have long made use of anonymous e-mail accounts.
Today these accounts are far more powerful.

- Yahoo and GMail both have 2GB of storage
- APIs allow this storage to be used as if it were a file system

Amazon’s Elastic Compute Cloud (EC2) and Simple Storage Service (S3) provide high-capability, little-patrolled services to anyone with a credit card

- EC2: 10 ¢/CPU hour (Xen-based virtual machines)
- S3: 10 ¢/GB-Month

With BGP, it’s possible to have “anonymous IP addresses.”

1. Announce BGP route
2. Conduct attack
3. Withdraw BGP address

Being used by spammers today

(http://www.nanog.org/mtg-0602/pdf/feamster.pdf)

Attacking the Investigator: AF techniques that exploit CFT bugs.

Craft packets to exploit buffer-overflow bugs in network monitoring programs like **tcpdump**, **snort** and **ethereal.**

Create files that cause EnCase to crash.

Successful attacks provide:

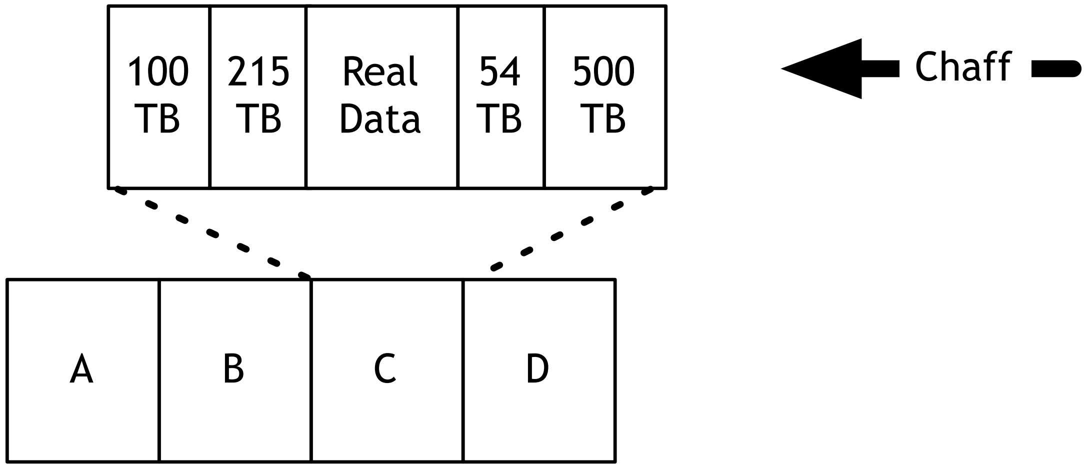
- ➡ Ability to run code on the forensic appliance
- ➡ Erase collected evidence
- ➡ Break the investigative software
- ➡ Leak information about the analyst or the investigation
- ➡ Implicate the investigator

Attacking the Investigator: Denial-of-Service Attacks against the CFT

Any CFT resource whose use is determined by input can be overwhelmed.

- Create millions of files or identities
- Overwhelm the logging facility
- Compression bombs — 42.zip

The clever adversary will combine this **chaff** with real data, e.g.:



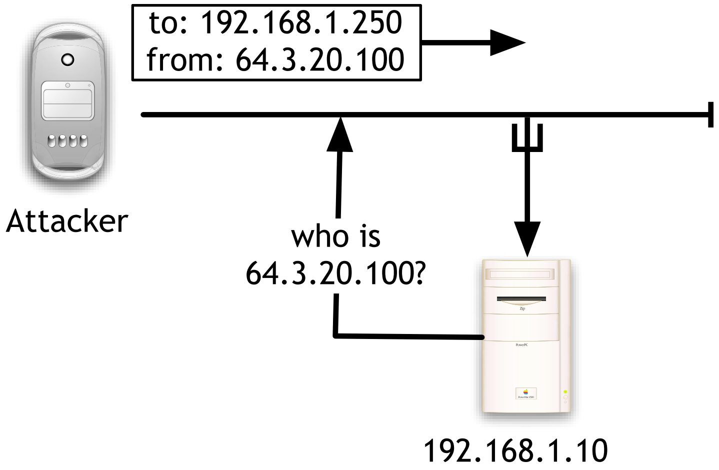
Anti-Forensic Tools can detect Computer Forensic Tools: cat-and-mouse.

SMART (Self-Monitoring, Analysis and Reporting Technology) drives report:

- Total number of power cycles
- Total time hard drive has been on

Network Forensics can be detected with:

- Hosts in “promiscuous” mode responding differently
  - — to PINGs.
  - — to malformed packets
  - — to ARPs
- Hosts responding to traffic not intended to them (MAC vs. IP address)
- Reverse DNS queries for packets sent to unused IP addresses



Countermeasures for Anti-Forensics

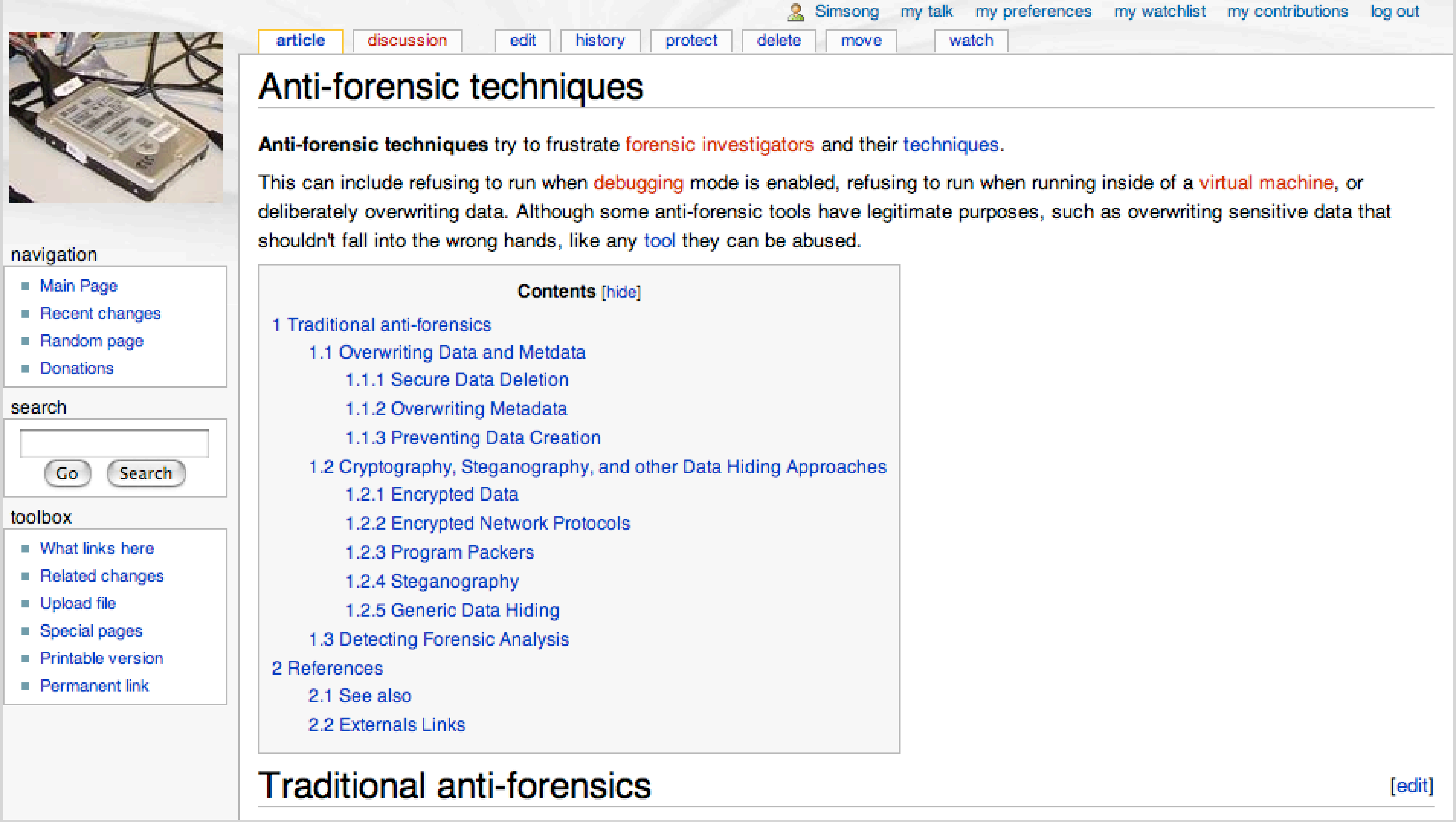
Improve the tools — many CFTs are poorly written.

Save data where the attacker can't get at it:

- Log hosts
- CD-Rs

Develop new tools:

- Defeat encrypted file systems with keyloggers.
- Augment network sniffers with traffic analysis



Anti-forensic techniques

Anti-forensic techniques try to frustrate forensic investigators and their techniques.

This can include refusing to run when debugging mode is enabled, refusing to run when running inside of a virtual machine, or deliberately overwriting data. Although some anti-forensic tools have legitimate purposes, such as overwriting sensitive data that shouldn't fall into the wrong hands, like any tool they can be abused.

Contents [hide]

- 1 Traditional anti-forensics
  - 1.1 Overwriting Data and Metdata
    - 1.1.1 Secure Data Deletion
    - 1.1.2 Overwriting Metadata
    - 1.1.3 Preventing Data Creation
  - 1.2 Cryptography, Steganography, and other Data Hiding Approaches
    - 1.2.1 Encrypted Data
    - 1.2.2 Encrypted Network Protocols
    - 1.2.3 Program Packers
    - 1.2.4 Steganography
    - 1.2.5 Generic Data Hiding
  - 1.3 Detecting Forensic Analysis
- 2 References
  - 2.1 See also
  - 2.2 Externals Links

Traditional anti-forensics

[edit]

Find out more at the Forensics Wiki: http://www.forensicswiki.org/

In Conclusion:

- Many forensic techniques in use today can be circumvented
- Circumvention tools are widely available
- Common approaches:
  - Overwriting data
  - Encrypting data
  - Anonymous identities & resources
  - Exploit bugs in computer forensic tools to hide
- New approaches:
  - Minimizing or eliminating memory footprints
  - Virtual machines
  - Direct attacks against computer forensic tools

http://www.simson.net/ref/2007/ICIW.pdf