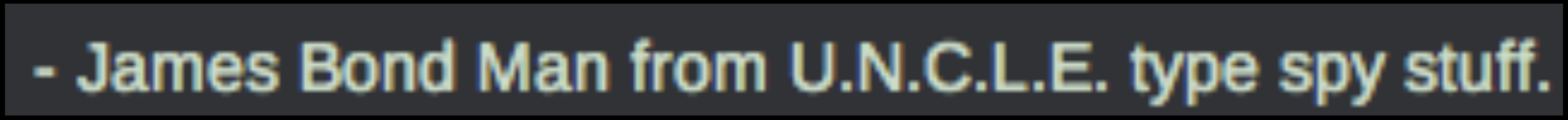
# Covert Post-Exploitation Forensics with Metasploit

Wesley McGrew
McGrewSecurity.com

Mississippi State University
National Forensics Training Center

From the DEF CON 19 CFP:



- James Bond Man from U.N.C.L.E. type spy stuff.

Okay, let's get sneaky...

# Covert

- without the subject’s knowledge

# Post-Exploitation

- after a remote compromise, local backdoor

# Forensics

- reconstructing data above and beyond what the subject anticipates

# Forensics and penetration testing/ other offensive operations

# For the forensics geeks...

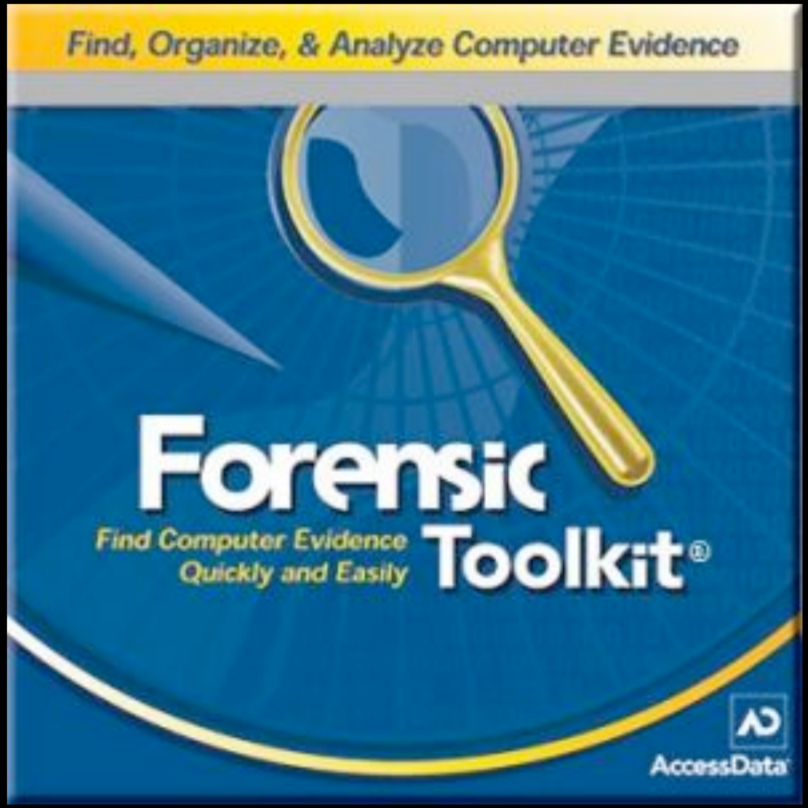
No subject location, no problem

Surreptitious acquisition and analysis

Familiar tools...

DFF
Digital
Forensics
Framework

PTK


Find, Organize, & Analyze Computer Evidence
Forensic
Toolkit®
Find Computer Evidence
Quickly and Easily
AD
AccessData

EnCase®

# For the penetration testing geeks...

Potential for more important data gathered per compromised system

“We don’t keep that data”

Multiple revisions of files, old data

Data carving

General purpose scripting

Stealthy!

# Typical Forensics Examination Scenarios

- Hardware seizure
- Authorized software agents
- On-site
- “Suspect”/Subject is aware

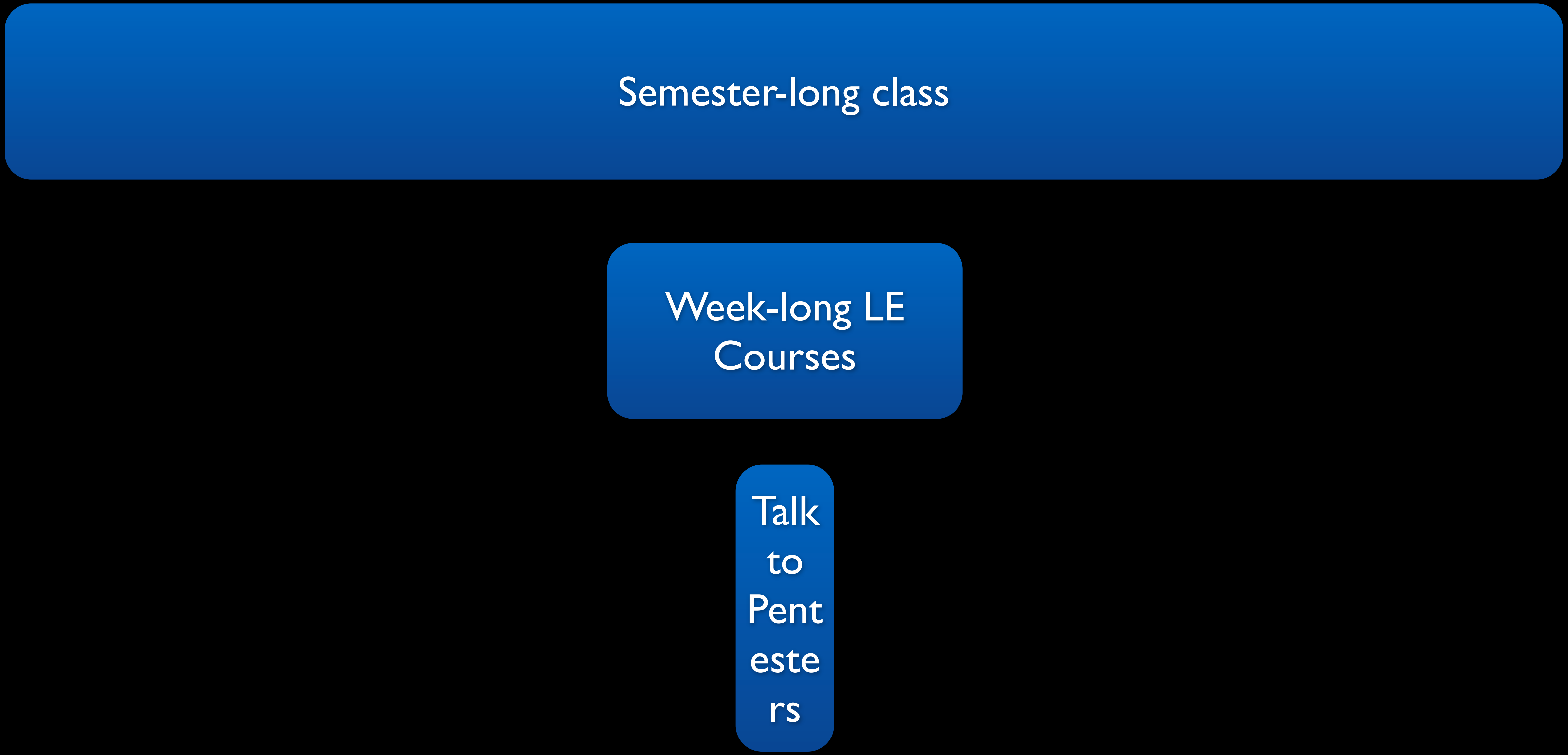
# Covert Remote Forensics

- Unaware Subject
- No known physical location?
  - Not a deal-killer.
- Remote imaging
- Remote block device access

# Ears perking up yet?

- Intelligence
- Penetration testers upping post-exploitation game
- Compliance
- Criminal

# Forensics for people who break things



Semester-long class

Week-long LE Courses

Talk to Pentesters

# File System Forensic Capabilities

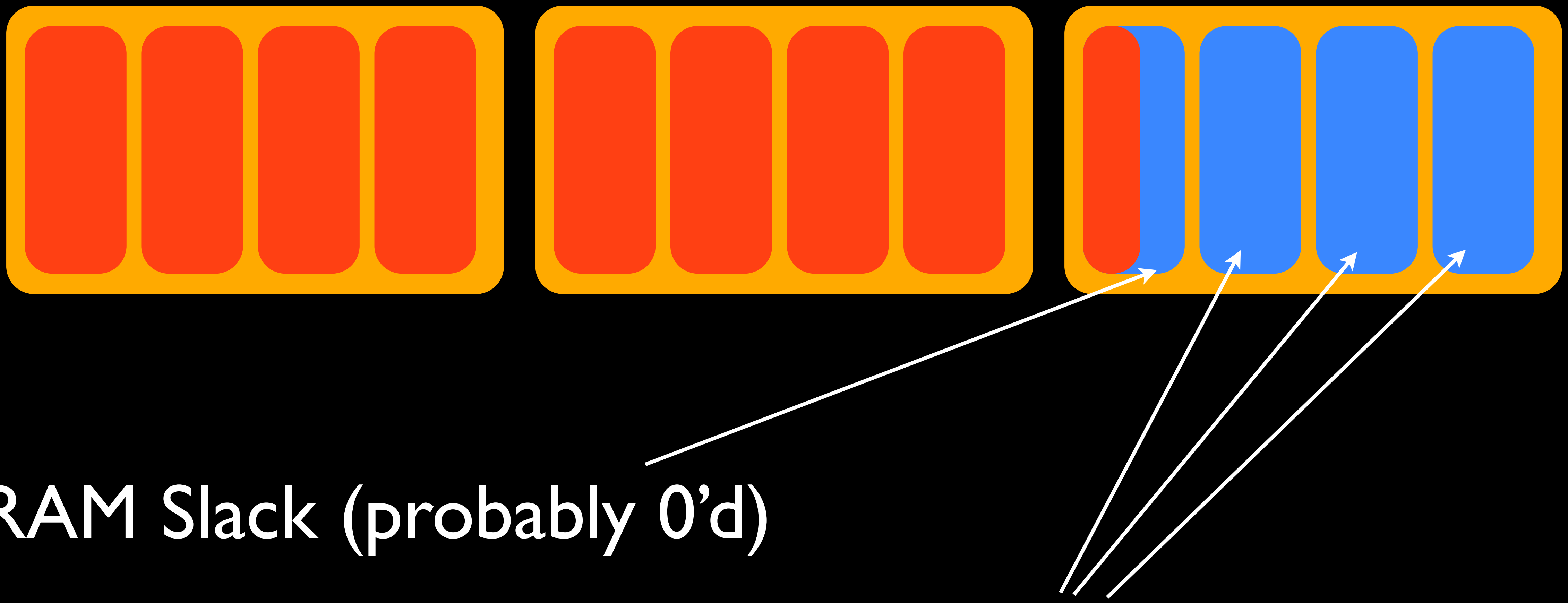
- Allocated files
- Deleted files
- Slack space
    - Disk/Volume
- Unallocated space
- Deletion vs. Formatting vs. Wiping
- Imaging

# Slack Space Example

Sector size: 512 bytes

Cluster size: 4 sectors

File size: 4150 bytes



RAM Slack (probably 0'd)

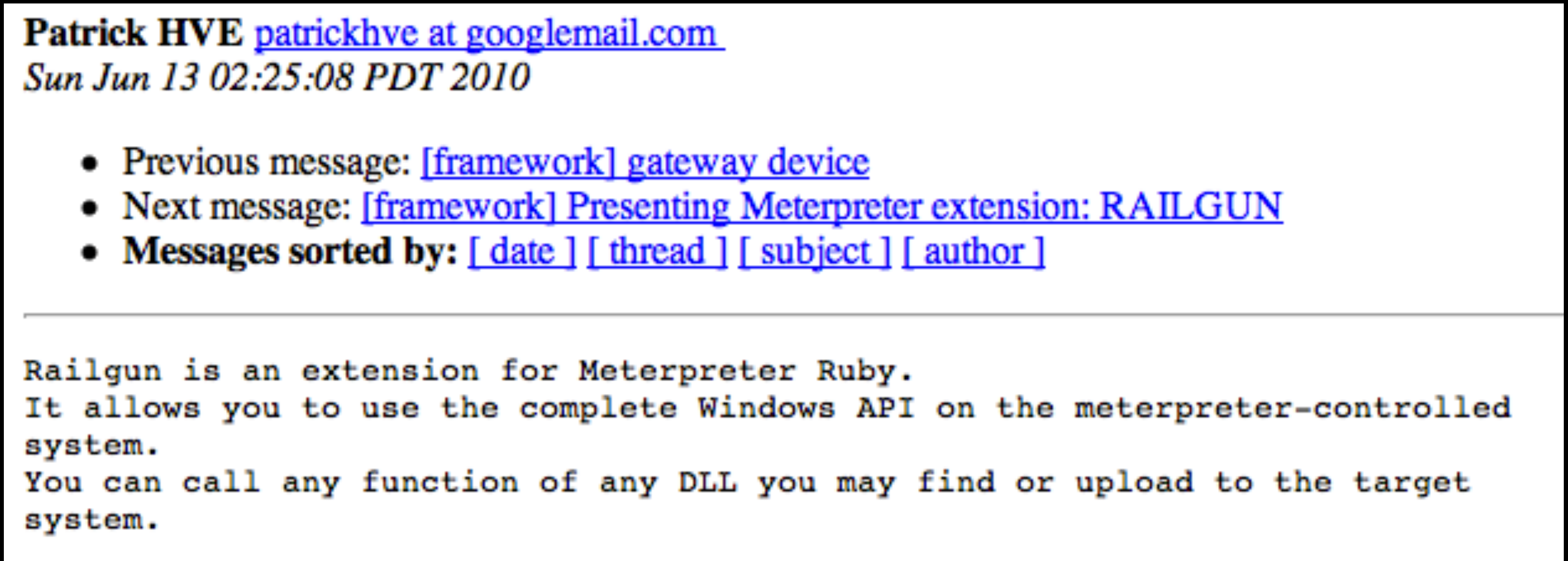
Disk Slack (potential goodies)

# Can’t I do this already?

- Load sleuth kit up onto the compromised target?
  - Probably will work but...
    - ...stomping on deleted files
    - ...not that stealthy
    - ...a little less slick than what I’m proposing:

# Enter Railgun

- “Patrick HVE” - Are you out there? Massive thanks!



**Patrick HVE** patrickhve at googlemail.com
*Sun Jun 13 02:25:08 PDT 2010*

- Previous message: [framework] gateway device
- Next message: [framework] Presenting Meterpreter extension: RAILGUN
- **Messages sorted by:** [ date ] [ thread ] [ subject ] [ author ]

---

```
Railgun is an extension for Meterpreter Ruby.
It allows you to use the complete Windows API on the meterpreter-controlled
system.
You can call any function of any DLL you may find or upload to the target
system.
```

# If we can call Windows API remotely...

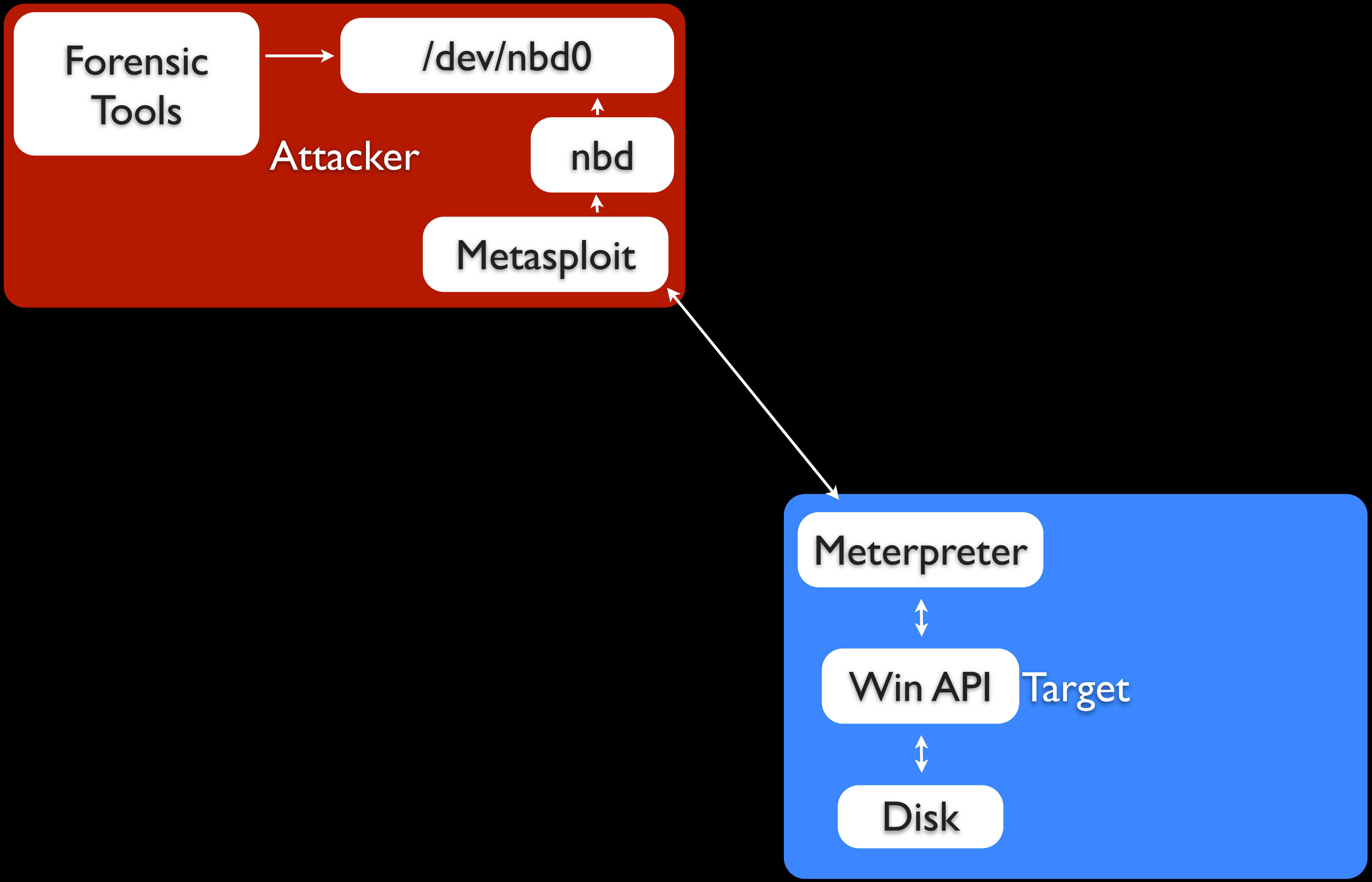
- ...then we can access physical/logical block devices directly
- ...which means we can read arbitrary sectors from the disk
- ...why not map remote block devices to local ones?

# Metasploit Post Modules

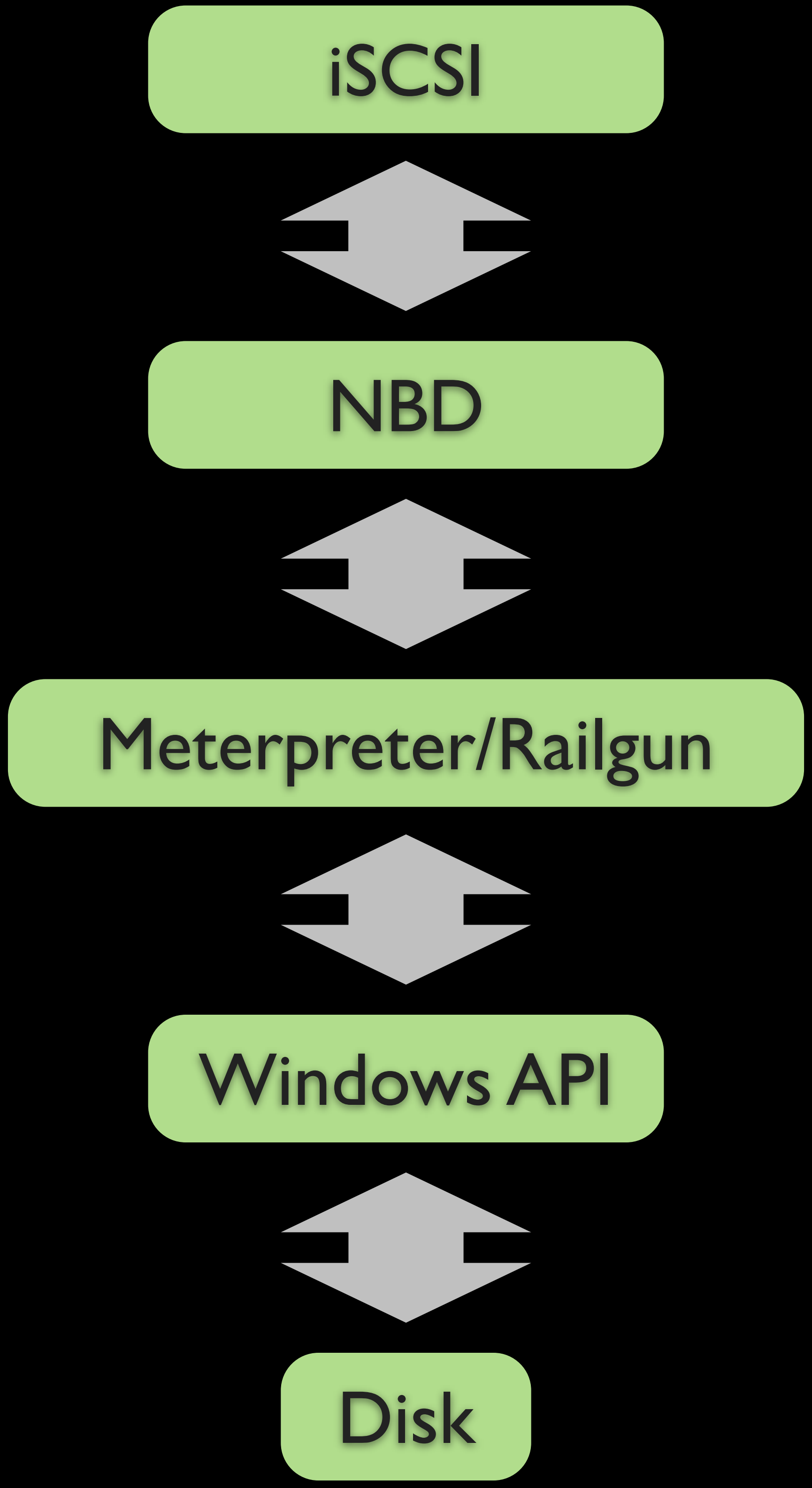
- **enum_drives.rb**
  - Helper/Support
- **imager.rb**
  - byte-for-byte imaging
  - Hashing
  - Split images
  - Cool, but..........

# nbd_server.rb!

- Run forensic tools locally, on local block devices that are mapped to remote block devices!
  - API calls made over meterpreter shell
  - NBD (Network Block Device)
    - Easy way to get programmatic block devices in Linux
  - Read-only (forensic write-blocking)
- Direct remote access with off-the-shelf/ commercial/open-source tools


Forensic Tools
/dev/nbd0
Attacker
nbd
Metasploit
Meterpreter
Win API
Target
Disk

# Stupid Protocol Tricks



iSCSI

NBD

Meterpreter/Railgun

Windows API

Disk

# Caveats and exercises for the reader

- Network
  - Speed
  - Stealth
- Cleaner/cross-platform implementation
  - Pure ruby iSCSI?

# Conclusions

- Go and wring more data out of systems!
- Builds capability for forensic examiners *and* penetration testers
- Encourage secure wiping

# Demos