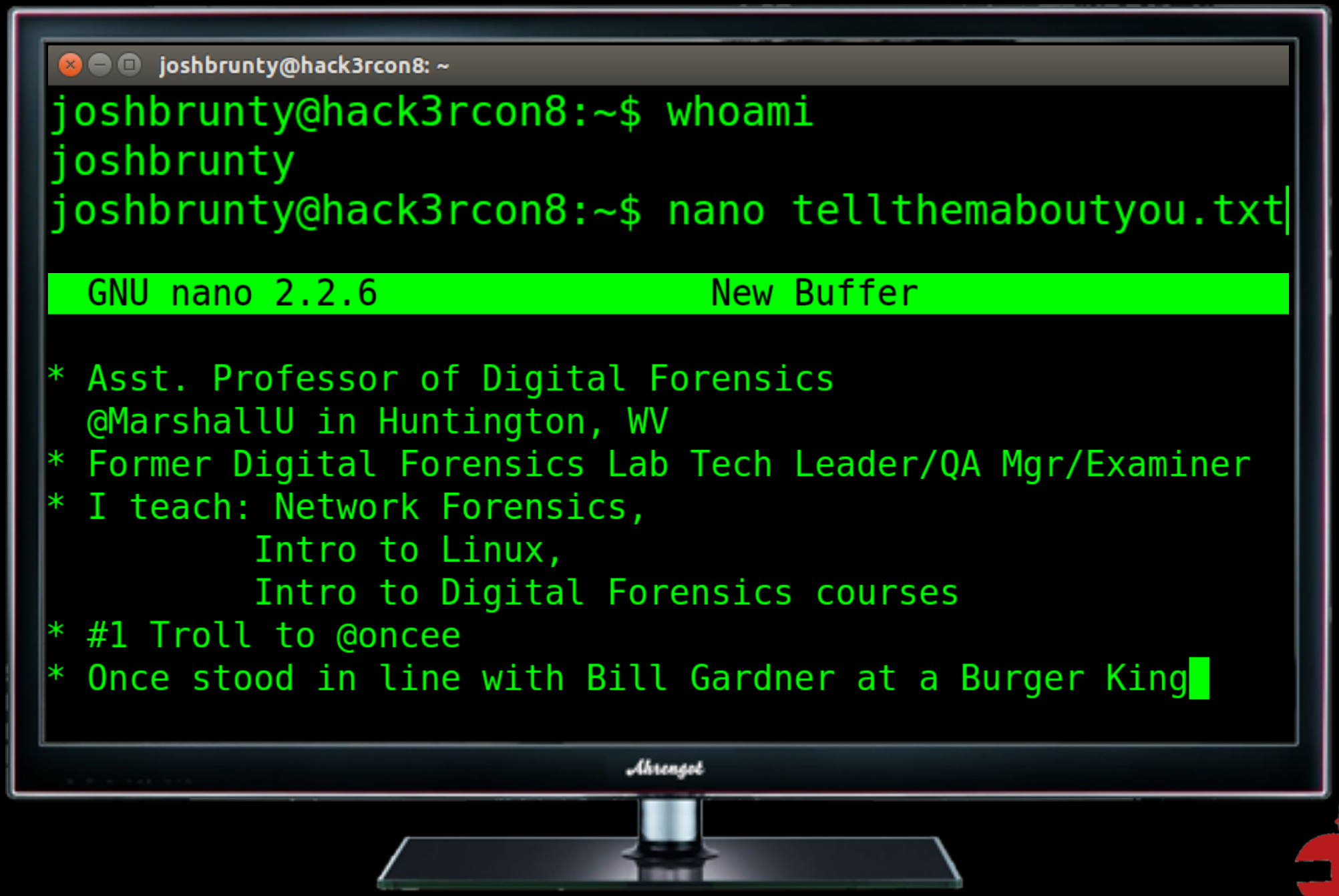
# Network Forensics using Kali Linux and SANS SIFT Workstation

**Josh Brunty**
Assistant Professor
Marshall University
josh [dot] brunty [at] marshall [dot] edu


DIGITAL FORENSICS
INFORMATION ASSURANCE


joshbrunty@hack3rcon8: ~
joshbrunty@hack3rcon8:~$ whoami
joshbrunty
joshbrunty@hack3rcon8:~$ nano tellthemaboutyou.txt
GNU nano 2.2.6 New Buffer
* Asst. Professor of Digital Forensics
@MarshallU in Huntington, WV
* Former Digital Forensics Lab Tech Leader/QA Mgr/Examiner
* I teach: Network Forensics,
Intro to Linux,
Intro to Digital Forensics courses
* #1 Troll to @oncee
* Once stood in line with Bill Gardner at a Burger King

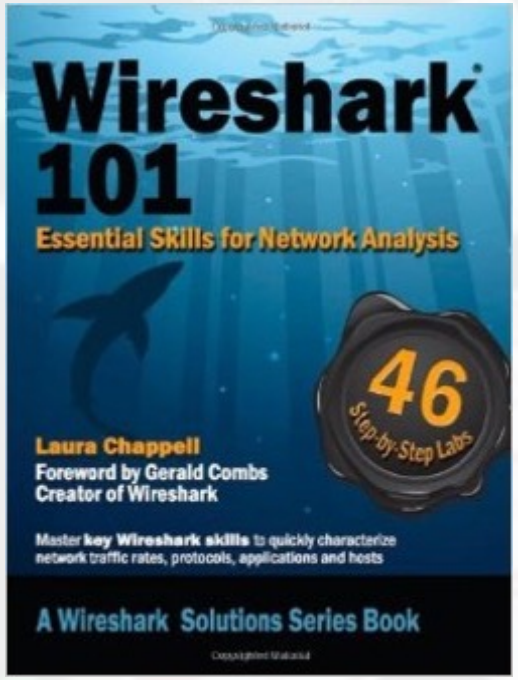
# *What we will need for this session…*

- Kali and/or SIFT Workstation
  - http://www.kali.org
  - https://digital-forensics.sans.org/community/downloads
- Bash terminal
- A stable internet browser
- Download course materials
  - https://github.com/joshbrunty/Hack3rCon8_NetworkForensics
  - PowerPoint, PCAP Files, Cheat Sheets
- Wireshark
  - www.wireshark.org
  - Version 2 (preferably)- already preloaded into Kali
  - Running in Linux (preferably SANS SIFT or Kali)
  - Linux Users: `apt-get install wireshark-qt`

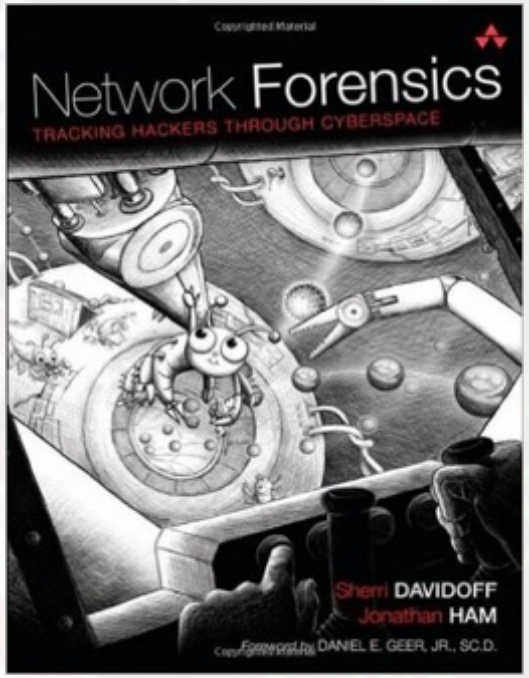
# *Session Overview*

- Lab #1
  - Standard packet investigation & file extraction
  - File used: evidence1.pcap
  - Tools: SIFT (Wireshark, grep/ngrep, NetworkMiner)
- Lab #2
  - Exploit Kit Investigation & Analysis
  - File used: evidence2.pcap
  - Tools: Kali (Wireshark, VirusTotal, NetworkMiner)
- Lab #3 (time permitting)
  - SysScout
  - File used: Collect Local Machine Info
  - Tools: SysScout.sh (GitHub Repository)

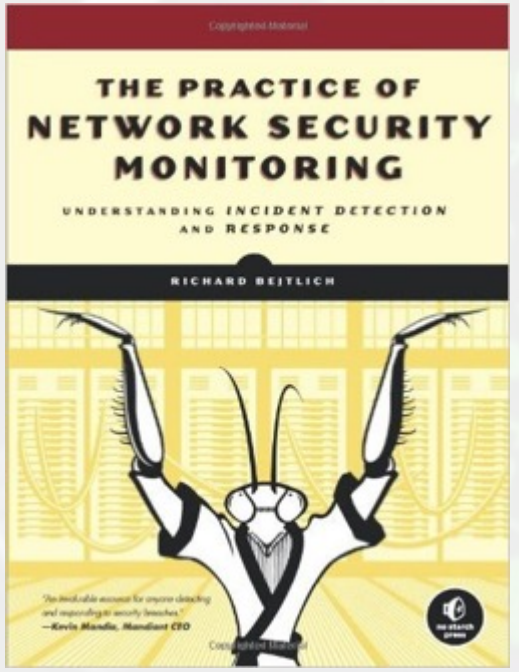
# Resources I'd Recommend…




http://a.co/0Zg87AK




http://a.co/dtRtKuA




http://a.co/agGV6Ht


http://a.co/iavdsQw

Hack3rCon 8 THE OCHO

# *Installing NetworkMiner In SIFT/Kali*

- **STEP 1: Install MonoUbuntu (also other Debian based distros like Xubuntu and Kali Linux)**
  - `sudo apt-get install mono complete`

- **STEP 2: Install NetworkMiner**
  - `wget www.netresec.com/?download=NetworkMiner -O /tmp/nm.zip`
  - `sudo unzip /tmp/nm.zip -d /opt/`
  - `cd /opt/NetworkMiner*`
  - `sudo chmod +x NetworkMiner.exe`
  - `sudo chmod -R go+w AssembledFiles/`
  - `sudo chmod -R go+w Captures/`

# *Lab #1*
# *“Ann’s Little Secret”*
# *Packet Investigation*

# *Lab #1- Packet Investigation*

After being released on bail, Ann Dercover has disappeared.  Fortunately, investigators were carefully monitoring her network activity before she skipped town.  “It is believed that Ann may have communicated with her secret lover, Mr. X, before she left” says the police chief.  “The packet capture may contain clues to her whereabouts

# *The Network:*

- Internal Network: 192.168.30.0/24
- DMZ: 10.30.30.0/24
- The “Internet”: 172.30.1.0/24 (note that this subnet will not yield any WHOIS information as this is a reserved subnet for non-routable traffic)

# *The Evidence:*

- evidence1.pcap
  - Packet Capture from Ann's Home Network
- Ann's Laptop MAC: 00:21:70:4D:4F:AE

# *The Investigation*

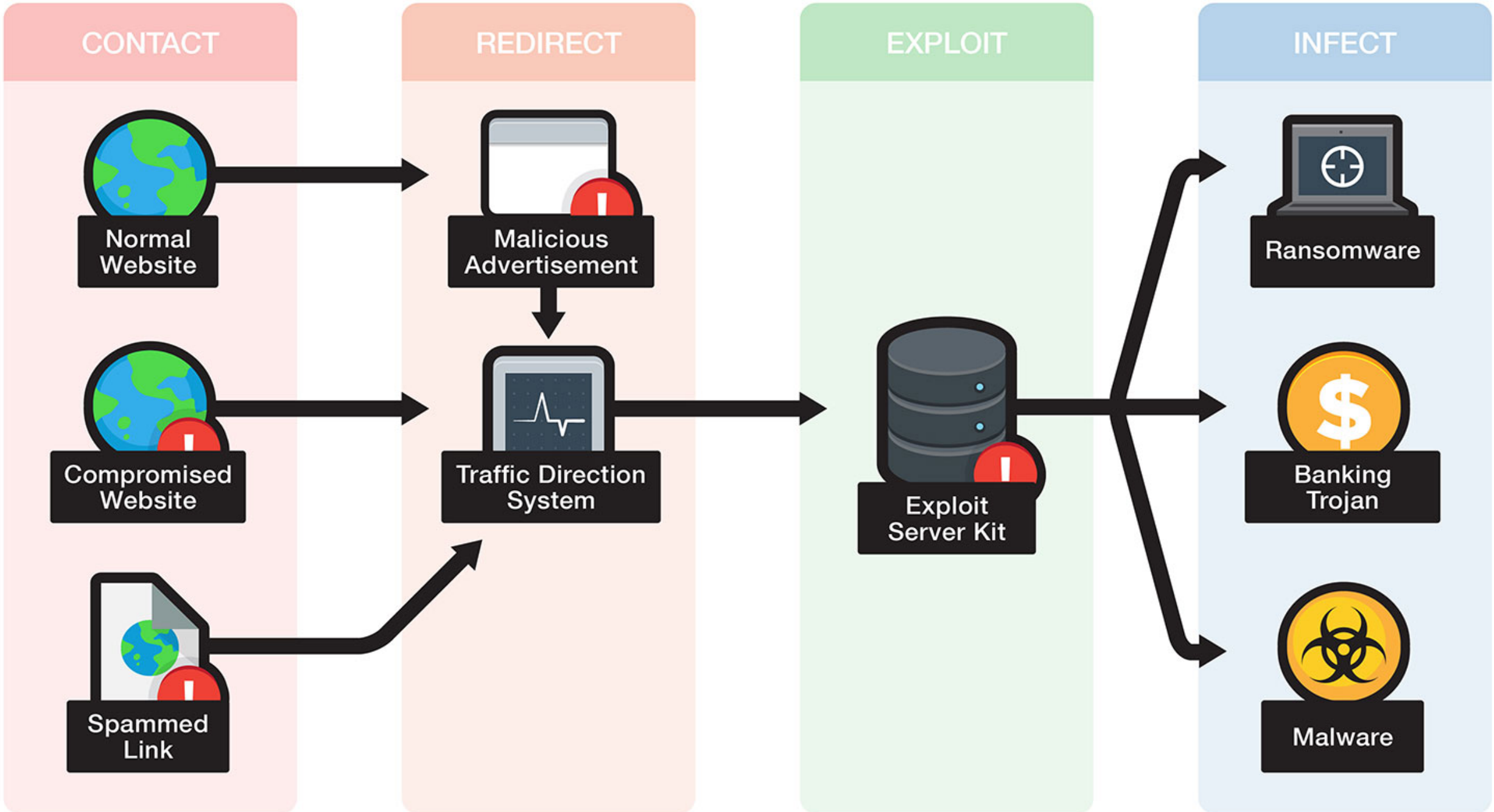
- Provide any online aliases or addresses that may have been used by the suspect
- Who did Ann communicate with? Provide a list of email addresses any any other identifying information
- Extract contents of Ann's conversations
- Did Ann transfer any files of interest?
- Are there any indicators of Ann's whereabouts?

# *Lab #2*
# *“Billie Went Nuclear”*
# *Exploit Kit Investigation*

# *Exploit Kits*

- What is an exploit kit?
  - Exploit kits are a type of malicious toolkit used to exploit security holes found in software applications (Adobe Reader, etc) for the purpose of spreading malware.
  - These kits come with pre-written exploit code and target users running insecure or outdated software applications on their computers.
  - While the process of becoming exploited by one of these kits will vary, the procedure usually goes a bit like this:

https://blog.malwarebytes.com/cybercrime/2013/02/tools-of-the-trade-exploit-kits/


CONTACT
REDIRECT
EXPLOIT
INFECT
Normal Website
Compromised Website
Spammed Link
Malicious Advertisement
Traffic Direction System
Exploit Server Kit
Ransomware
Banking Trojan
Malware

# *Exploit Kits*

- The Process…
  - A victim visits a website whose server has been hacked by cybercriminals.
  - The victim is redirected through various intermediary servers
  - The victim lands at a rogue server hosting the exploit kit
  - The exploit kit gathers information on the victim and determines the exploit to deliver
  - Exploit is sucessfully/unsuccessfully delivered
  - If exploit succeeds, a malicious payload (custom malware program) is downloaded to the victim's computer and executed.

https://blog.malwarebytes.com/cybercrime/2013/02/tools-of-the-trade-exploit-kits/

9 NOV 2016 NEWS

# Antivirus Fails to Stop Ransomware 100% of the Time

Tara Seals US/North America News Reporter, Infosecurity Magazine
Email Tara

**Traditional antivirus fails to stop ransomware 100% of the time.**

That's according to a recent survey from Barkly of companies that suffered successful ransomware attacks during the last 12 months. A full 100% reported they were running antivirus at the time of the attack.

And antivirus wasn't the only security solution that came up short. Victims reported that 95% of the attacks bypassed the victim's firewall(s); 77% of the attacks bypassed email filtering; 52% of the attacks bypassed anti-malware; and 33% of the attacks were successful even though the victim had conducted security awareness training.

Not a great track record. But what's baffling is the finding that most companies don't alter their approaches after a ransomware attack.



## Why Not Watch?

http://www.infosecurity-magazine.com/news/antivirus-fails-to-stop-ransomware

Hack3rCon 8 THE OCHO

*THE BOTNETS OF MADISON COUNTY —*

# Indiana county government shut down by ransomware to pay up

Commissioner of Madison County says insurance company advised paying ransom.

SEAN GALLAGHER - 11/8/2016, 1:17 PM

http://arstechnica.com/security/2016/11/indiana-county-government-shut-down-by-ransomware-to-pay-up/

WEB TECH CYBERSECURITY

# Crunchyroll is back online after a malware attack

1

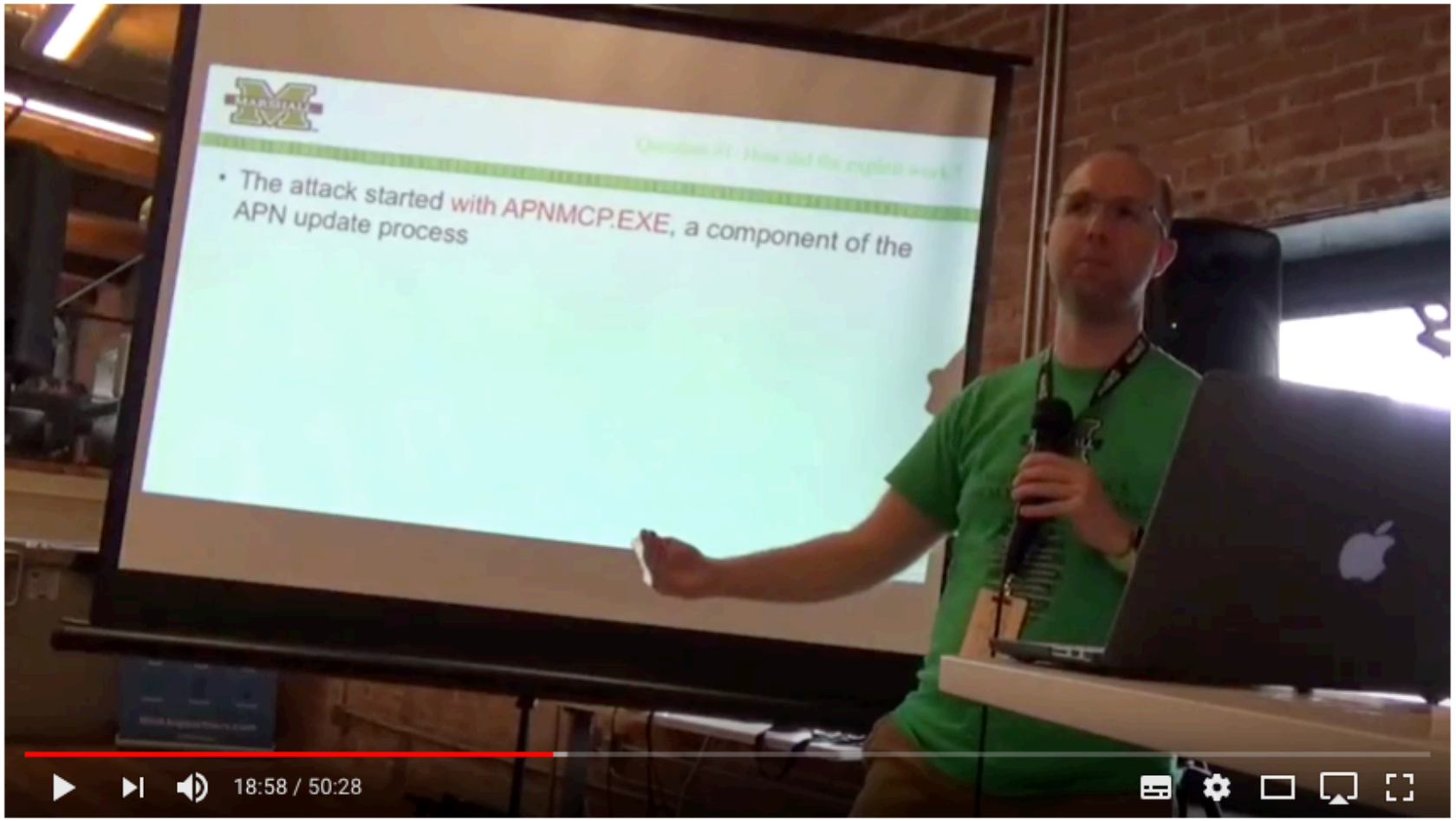
*The site was taken offline after users were prompted to download malware*

by Andrew Liptak | @AndrewLiptak | Nov 4, 2017, 1:22pm EDT






https://www.theverge.com/2017/11/4/16605488/crunchyroll-back-online-malware-attack-cybersecurity-anime




BSidesKC 2017 - Track 1 - Josh Brunty – PUPs to Pwn: Attack vectors of the newest waves of bloatware

https://youtu.be/MT_UhU_Hwjg

# *Lab #2- Billie Went Nuclear (Exploit Kit)*

- At your DC-based company (Clinton, Inc.) Security Operations Center (SOC), an analyst received a call from Billie Gardner, who is an executive assistant for your Chief Executive Officer (CEO), William “Billy” Clinton at the UK Office.
- While searching for a tasty steak dinner location for his boss Billy, Billie described the computer as “acting funny” and “files inaccessible”.  He also stated that the desktop wallpaper had been changed and said something about “ransom” and “paying up”

# Lab #2- Billie Went Nuclear

# *Lab #2- Billie Went Nuclear*

- At the same time One of the other analysts is investigating a snort alert that came in at the exact same time.
- Fortunately, that location has full packet capture, and the analyst retrieved a .pcap of network traffic (evidence2.pcap) from the associated IP address.
- You've been asked to take a look and determine what exactly happened and what must be done to mitigate further damage to the company's network.

# *Lab #2- Billie Went Nuclear*

- You review the pcap and check the other analyst's report.  First, we need to double-check the following:
  - Date and time of the activity
  - IP address of computer
  - Host name of computer
  - MAC address of computer
  - IP address and domain name that generated the traffic

# *Lab #2- Billie Went Nuclear*

- Traffic indicates the user was web browsing. With this in mind, you try to determine:
  - What website the user looked at before the malicious traffic
  - If a malware payload was sent that could possibly infect the user's computer

# *Lab #3*
# *“SysScout”*
# *Collecting Linux/Mac Local System Info*

# *Lab #3- SysScout*

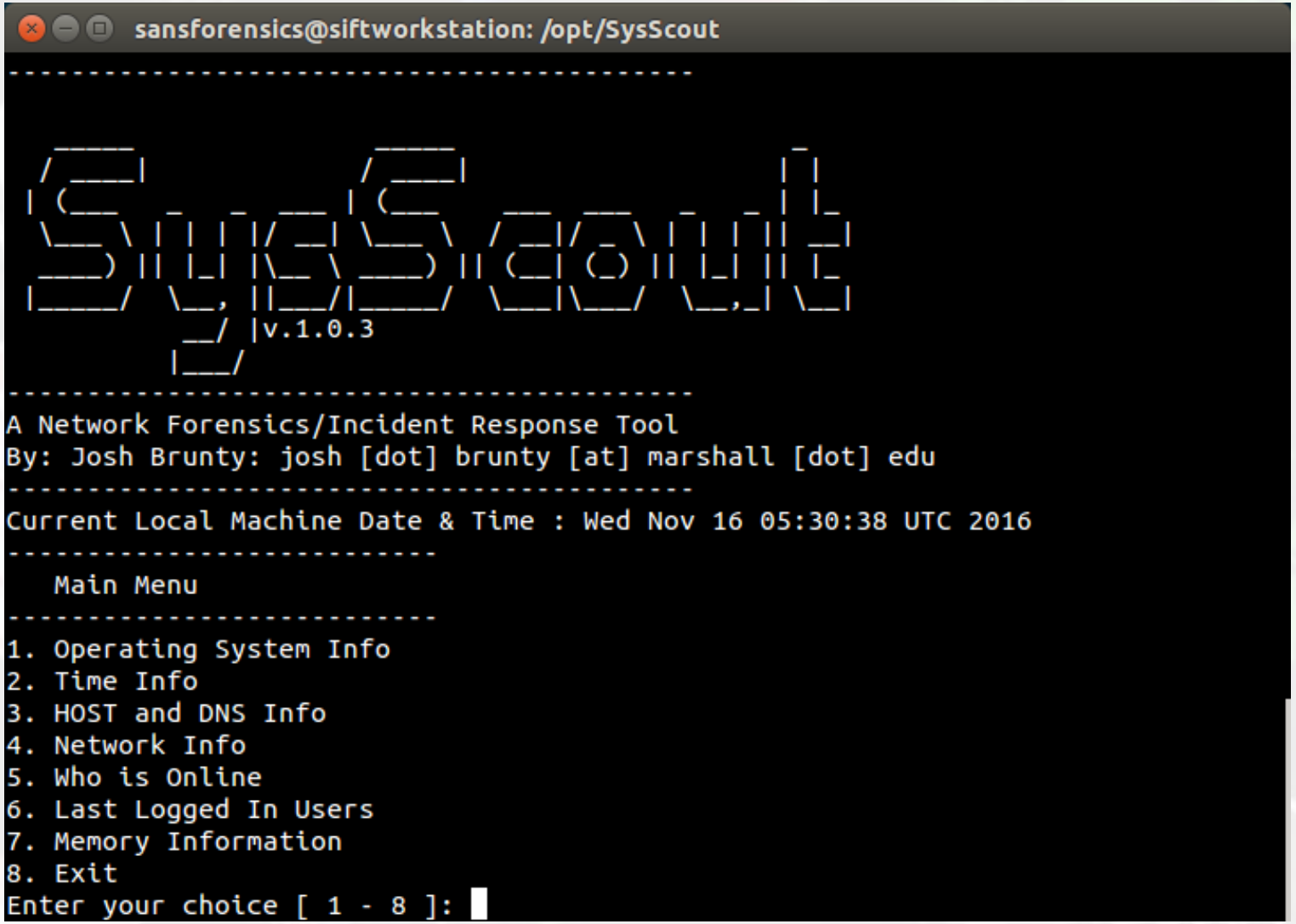
- Sometimes the need arises to collect intel on a specific Linux Machine/Server
- If you're memory is like mine, I only retain about 0.00000000001% of terminal commands
- I also loathe using Python Scripts that require about 1600 add-on modules to be installed and/or imported

# *Lab #3- SysScout*

- SysScout is a simple, fully contained shell script that was built to simplify commonly used terminal commands I was commonly using in Network Forensics/Incident Response Investigations.
- It's easy and simple.
- Download link:
  - http://www.github.com/joshbrunty/SysScout

*Use the menu structure in this script to make your own bash script for your own tasks

# Lab #3- SysScout



# Network Forensics using Kali Linux and SANS SIFT Workstation

**Josh Brunty**
Assistant Professor
Marshall University
josh [dot] brunty [at] marshall [dot] edu


DIGITAL FORENSICS
INFORMATION ASSURANCE

**SecureWV/HackerCon 2016**