Network Forensics Workshop with NetworkMiner

Erik Hjelmvik
<erik.hjelmvik [at] gmail.com>

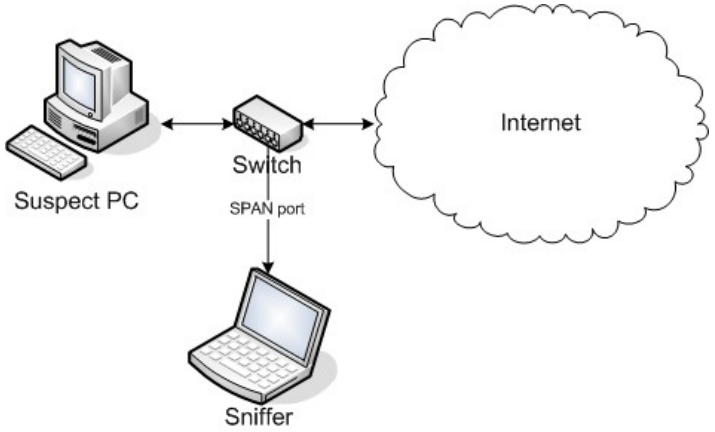
High Tech Crime Experts Meeting 2009
Europol Headquarters in The Hague, The Netherlands

When Law Enforcement need to perform Network Forensics

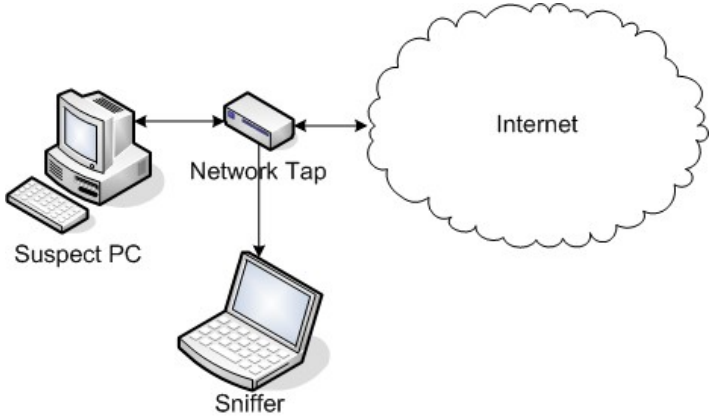
- Lawful Interception of a suspect's Internet connection
- When performing *digital evidence collection* from a stand alone computer
  - Acquire data in transit (network traffic dump)
  - Acquire data in use (RAM image)
  - Acquire data at rest (hard drive image)
- A corporate incident response team has discovered network traffic that violates the law

Connecting a Network Sniffer

- SPAN/mirror port
  - Re-configuration of switch
  - Free port on switch



- Network Tap
  - Special hardware
  - No configuration



Capturing Network Traffic

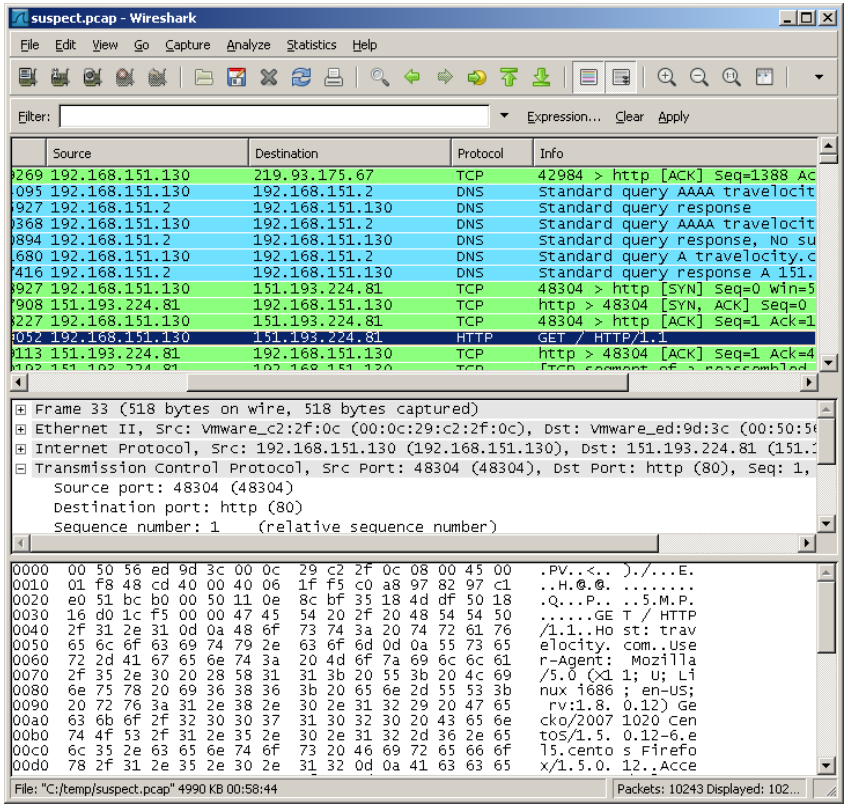
```
#
# Capture traffic to and from IP 213.1.2.3
# Create new file for every 100MB
# Dump traffic to file ”wiretap.pcap”
#

> dumpcap -i 1 -f "host 213.1.2.3" -w
  wiretap.pcap -b filesize:100000
```

Analyzing Network Traffic

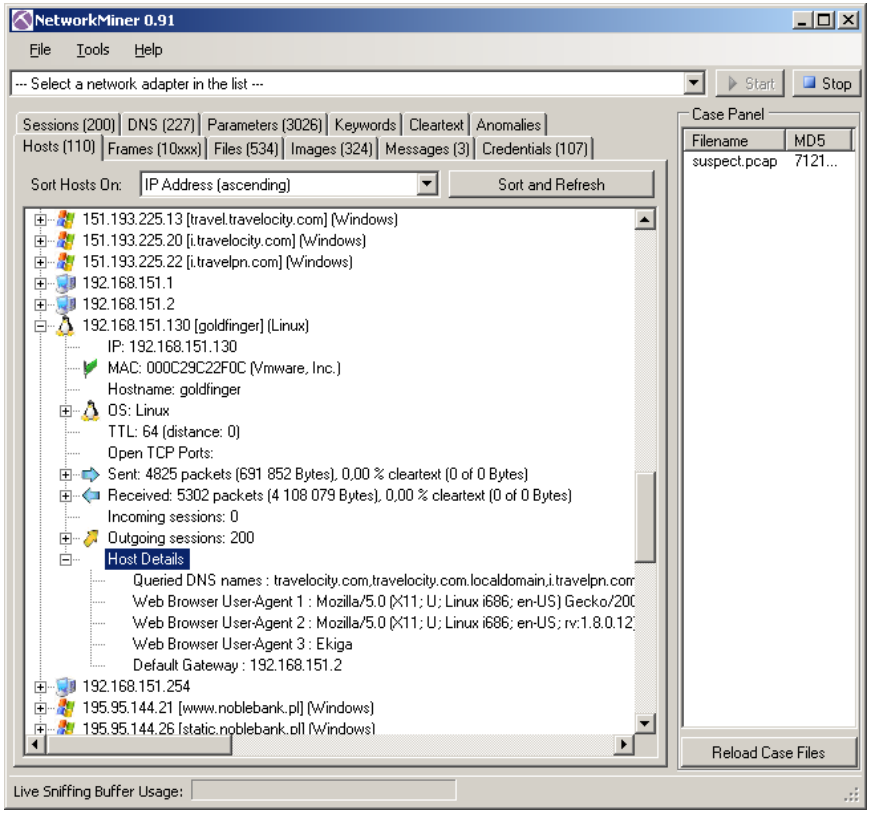
Wireshark

http://www.wireshark.org/



NetworkMiner

http://networkminer.sourceforge.net/



Case #1 – Puzzle 1

http://forensicscontest.com/2009/09/25/puzzle-1-anns-bad-aim
file: evidence.pcap

An employee, Ann Dercover, is suspected of being a secret agent working for the competitor. An unexpected laptop briefly appeared on the company wireless network. Staff hypothesize it may have been someone in the parking lot, because no strangers were seen in the building. Ann's computer, used AOL Instant Messenger (using the Oscar protocol) to send messages over the wireless network to this computer.

- What IP address did Ann's computer have?
- What IP address did the stranger's computer have?
- What operating system did the stranger's computer have?
- What is the brand of the stranger's computer, if you trust the MAC address of his wireless network card?
- What is the filename of the file sent over IM to the wireless laptop?
- What type of information did the sent file contain?
- What AOL messenger username does Ann's contact use?
- Where do Ann and the external party plan to meet?

Case #2 – Puzzle 2

http://forensicscontest.com/2009/10/10/puzzle-2-ann-skips-bail
file: evidence02.pcap

After being released on bail, Ann Dercover disappears! Fortunately, investigators were carefully monitoring her network activity before she skipped town. "We believe 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."

- What is Ann's email address?
- What is the email address of Ann's secret lover?
- What is Ann's email password?
- What two items did Ann tell her secret lover to bring?
- Where do Ann and her secret lover plan to meet up?

Case #3 – DFRWS

http://www.dfrws.org/2008/challenge/submission.shtml
file: suspect.pcap

An employee named Steve Vogon is suspected of having illegal contacts with external parties. Steve is believed to have used his personal Linux laptop on the corporate network for his suspicious activity.

- What IP address and hostname does Steve Vogon's Linux computer have?
- What evidence do you have to assume that this computer is running Linux?
- What Google searches did Steve Vogon perform?
- What message did the email contain that Steve Vogon sent from his Gmail account?
- How did Steve find the email address to which he sent his email?
- One web page opened by Steve contains a map, what region does the map show?

DFRWS
DIGITAL FORENSIC RESEARCH WORKSHOP

Case #4 – HoneyNet.org

http://old.honeynet.org/scans/scan28/
file: day1.log

An old Sun Solaris machine (192.168.100.28), called "the victim machine", was hacked through a vulnerability in the CDE Subprocess Control Service on TCP port 6112.

- What IP address did the attack come from?
- After compromise, what files did the attacker download to the compromised victim machine using FTP?
- What usernames and passwords did the attacker use for his FTP connections from the victim machine?
- Why did the attacker run FTP rather than HTTP to perform his initial downloads?
- What file was later on downloaded using the HTTP protocol?
- What web server brand is this HTTP server running?
- What is the full DNS name of the IRC server to which the victim machine connected?
- What Nick-name is the attacker using when connecting the victim machine to the IRC server?

Case #5 – TaoSecurity

http://taosecurity.blogspot.com/2009/02/sample-lab-from-tcpip-weapons-school-20.html
file: case09.pcap

Samantha Athew receives an email to her personal gmail address with an attached HTML file claimed to be "a new cool Web page". She reports that after opening the attached HTML file her computer started behaving suspiciously.

- What is Samantha's email address?
- Apart from Samantha's email account, what other email address is used in the captured traffic?
- The attached “cool web page” contains a reference to an image, where (at what network location) is this image?
- What happens when Samantha opens the attached HTML file?

  Hint: an attack is carried out that could give the attacker access to files on Samantha’s computer
- The victim machine visits three SSL-encrypted websites that have self-signed certificates, what IP-addresses are those webservers residing on?

Bonus Case – DefCon 11

https://www.openpacket.org/capture/show/45
file: dump.eth0.1059726000

This capture is not a case to be investigated, just REAL traffic from the hacker conference DefCon

- The user of 192.168.16.200 has logged into his web based MS Exchange email interface. What username and password is he using?
- A Defcon visitor downloaded a network vulnerability scan report from neptnet.com. What single IP address was that vulnerability scan performed against according to the report?
- A journalist at The New Your Times has sent an email using unencrypted SMTP. In which organization does the recipient of the email work?
- A user claims in an AOL Instant Message that “there is more guys in skirts then women” at Defcon. What is the hostname of this users computer and what is the username to which the message is sent?
- One DefCon visitors downloaded an image showing a computer from Sun Microsystems on a red chair. What does the Post-it note on the Sun machine say?
- What IP address does the user have who downloads the wifi-monitoring tool NetStumbler?
- One user downloads the source code to the legacy Denial-of-Service tool “WinNuke”, what is the hostname of the user's computer?

Answers to Case Questions

Case #1 – Puzzle 1

Q: What IP address did Ann's computer have?
A: 192.168.1.158

Q: What IP address did the stranger's computer have?
A: 192.168.1.159

Q: What operating system did the stranger's computer have?
A: Windows XP. See OS fingerprinting results by Ettercap, P0f and Satori as well as Web-browser user agent "Windows NT 5.1" in "Host Details".

Q: What is the brand of the stranger's computer, if you trust the MAC address of his wireless network card?
A: "Dell".

Q: What is the filename of the file sent over IM to the wireless laptop?
A: "recipe.docx". See Files tab

Q: What type of information did the sent file contain?
A: A "recipe for disaster". Open the .docx file in a MS Word or rename the .docx file to .zip and open up "recipe.docx\word\document.xml"

Q: What AOL messenger username does Ann's contact use?
A: "Sec558user1"

Q: Where do Ann and the external party plan to meet?
A: In Hawaii (see messages tab)

Case #2 – Puzzle 2

Q: What is Ann's email address?
A: sneakyg33k@aol.com

Q: What is the email address of Ann's secret lover?
A: mistersecretx@aol.com

Q: What is Ann's email password?
A: 558r00lz

Q: What two items did Ann tell her secret lover to bring?
A: Fake passport and a bathing suit.

Q: Where do Ann and her secret lover plan to meet up?
A: Playa del Carmen in Mexico

Case #3 – DFRWS

Q: What IP address and hostname does Steve Vogon's Linux computer have?
A: 192.168.151.130 and "goldfinger" (See hosts list)

Q: What evidence do you have to assume that this computer is running Linux?
A: Web Browser User-Agent (in "Host Details" for 192.168.151.130) shows Linux i686 and Satori fingerprints the host's TCP/IP stack as well as DHCP stack as being from a Linux 2.6 kernel.

Q: What google searches did Steve Vogon perform?
A: "overseas credit card payments" and "hurricane". Sort parameters tab on param name and look for parameter "q".

Q: What message did the email contain that Steve Vogon sent from his gmail account?
A: "Hello, Can you please tell me what the minimum balance requirement is for opening an overseas account at your bank? Thank you, Steve K. Vogon"

Q: How did Steve find the email address to which he sent his email?
A: In the "index.jsp.3DD784EE.html", found by doing a keyword search for "investors@noblebank.pl"

Q: One web page opened by Steve contains a map, what region does the map show?
A: The caribbean sea, see "TT_caribb_map_260x195.gif" in Images tab or Files tab.

Case #4 – HoneyNet.org

Q: What IP address did the attack come from?
A: 61.219.90.180. See Sessions tab, where the first session goes from this host to the victim machine on TCP port 6112.

Q: After compromise, what files did the attacker download to the compromised victim machine using FTP?
A: "ipv6sun", "dlp", "111085-02.zip" (patch of the vulnerability), "solbnc" (IRC bot "psyBNC" used as a C&C/backdoor) and "wget"

Q: What usernames and passwords did the attacker use for his FTP connections from the victim machine?
A: bobzz/joka and anonymous/root@zoberius.example.net.mx

Q: Why did the attacker run FTP rather than HTTP to perform his initial downloads?
A: There was no HTTP client on the compromized machine, which was why "wget" was downloaded

Q: What file was later on downloaded using the HTTP protocol?
A: "sol.tar.gz.x-tar"

Q: What web server brand is this HTTP server running?
A: Apache (version 1.3.26). See host details for 62.211.66.53

Q: What is the full DNS name of the IRC server to which the victim machine connected?
A: irc.stealth.net

Q: What Nick-name is the attacker using when connecting the victim machine to the IRC server?
A: "Dj`bobz`" (see Host details for 192.168.100.28)

Case #5 – TaoSecurity

Q: What is Samantha's email address?
A: samanthaatews@gmail.com (messages tab)

Q: Apart from Samantha's email account, what other email address is used in the captured traffic?
A: samuelatews@gmail.com (see Messages tab, parameters for frame 3117 or file from frame 3120)

Q: The attached "cool web page" contains a reference to an image, where (at what network location) is this image?
A: \\10.1.1.6\share2\1.jpg (see cool_web_page.html)

Q: What happens when Samantha opens the attached HTML file? Hint: an attack is carried out that could give the attacker access to files on Samantha's computer
A: Her computer connects to 10.1.1.6 using SMB (NetBiosSessionService) on port 139 authenticating her with her username "samantha" and encrypted password. This computer in turn connects back to Samanthas computer using the same protocol (on port 445) and credentials. This is an SMB relay attack.

Q: The victim machine visits three SSL-encrypted websites that have self-signed certificates, what IP-addresses are those webservers residing on?
A: 85.25.145.98, 62.141.58.13 and 66.230.230.230 (inspect the .cer certificates in "files" tab)

Bonus Case – DefCon 11

Q: The user of 192.168.16.200 has logged into his web based MS Exchange email interface. What username and password is he using?
A: gvallem and canicas (frame 3502)

Q: A Defcon visitor downloaded a network vulnerability scan report from neptnet.com. What single IP address was that vulnerability scan performed against according to the report?
A: 192.168.0.77, file can be found under the Files tab in frame 14152 (the file is named "report.html")

Q: A journalist at The New Your Times has sent an email using unencrypted SMTP. In which organization does the recipient of the email work?
A: The U.S. Senate (frame 44636)

Q: A user claims in an AOL Instant Message that "there is more guys in skirts then women" at Defcon. What is the hostname of this users computer and what is the username to which the message is sent?
A: SRAYMOND and zoitzia (frame 73580)

Q: One DefCon visitors downloaded an image showing a computer from Sun Microsystems on a red chair. What does the Post-it note on the Sun machine say?
A: "PLEASE STEAL ME!" (frame 79870)

Q: What IP address does the user have who downloads the wifi-monitoring tool NetStumbler?
A: 192.168.16.230 (frame 184505)

Q: One user downloads the source code to the legacy Denial-of-Service tool "WinNuke", what is the hostname of the user's computer?
A: "hazzard2". See files tab for "winnuke.c.txt" (frame 291861)