



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Digital Forensics Analysis (ACCA7031_LON)

Lecture 8

Network Forensics and Cyber-Incident Investigation

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk

Content covered

- Introduce Network Forensics
- Explain the Order of volatility (OOV) in cyber forensics
- Explain Live acquisitions (RAM)
- Explain network traffic capturing and the examination process
- Detail techniques and approaches for network and security logs examinations
- Enumerate network forensics tools

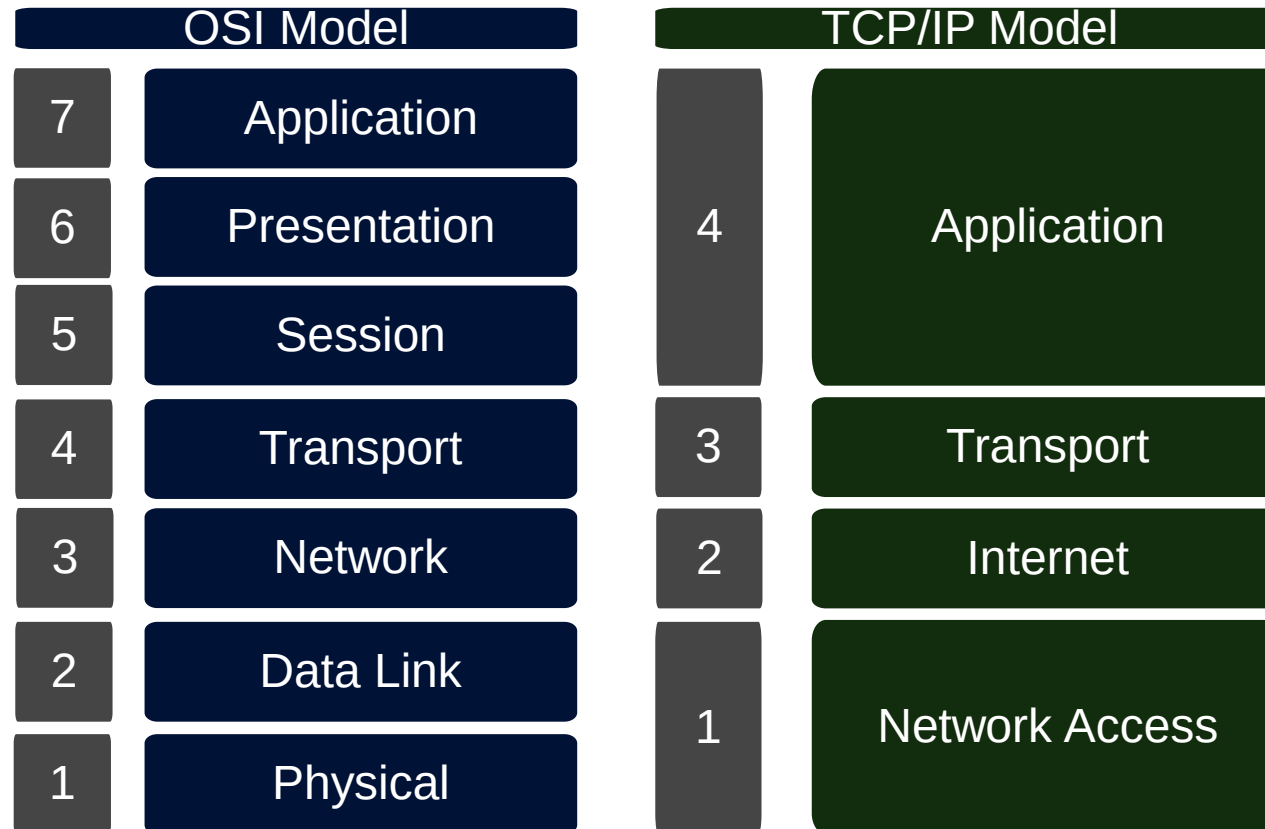
Objectives

- Understand Internet and Networking fundamentals for cyber forensics
- Understand network forensics
- Understand traffic analysis and investigation techniques
- Understand the Order of Volatility and the importance of live data acquisition in cyber forensics
- Aware of the used network Forensics tools

Internet Fundamentals

- Internet = Collection of networks
- Internet Service Provider (ISP)
 - Internet entry point
 - Username and password
- Domain Name Service (DNS)
 - Translate IP addresses to named addresses or vice versa
- Common software
 - Web browsers, e-mail clients, etc.
- Internet protocols
- TCP/IP (default Internet protocol),
 - TCP - UDP - FTP

OSI and TCP/IP models



Internet Fundamentals (cont.)

- Addressing (IPv4)
 - 32-bit long divided into four groups of 8 bits
 - Binary representation
 - Dotted quad (205.55.29.170)
- NAT - Network Address Translation
 - Translates IP addresses
- Problems with available IP addresses

Internet Fundamentals (cont.)

Class	Value of 1 st Octet	High Order Bit	Default Subnet Mask	Possible Network	Hosts per Network	Private IP Address Range
A	0-127	0	255.0.0.0 or /8	$2^{8-1}=128$	$2^{8-2}=16777214$	10.0.0.0 to 10.255.255.255
B	128-191	10	255.255.0.0 or /16	$2^{16-2}=16384$	$2^{16-2}=65534$	172.16.0.0 to 172.31.255.255
C	192-223	110	255.255.255.0 or /24	$2^{24-3}=2097152$	$2^{24-2}=254$	192.168.0.0 to 192.168.255.255
D	224-239	1110	-			
E	240-255	1111	-			

Note:

0.0.0.0/8 reserved for default route

127.0.0.0/8 reserved for loopback addresses

169.254.0.0/16 reserved for link-local address. This range also called automatic private IP addressing

Key Network Devices

- Switches
- Routers
- Firewalls
- Network intrusion detection and prevention systems
- Web proxy servers
- Domain controllers or authentication servers
- DHCP server
- Application servers

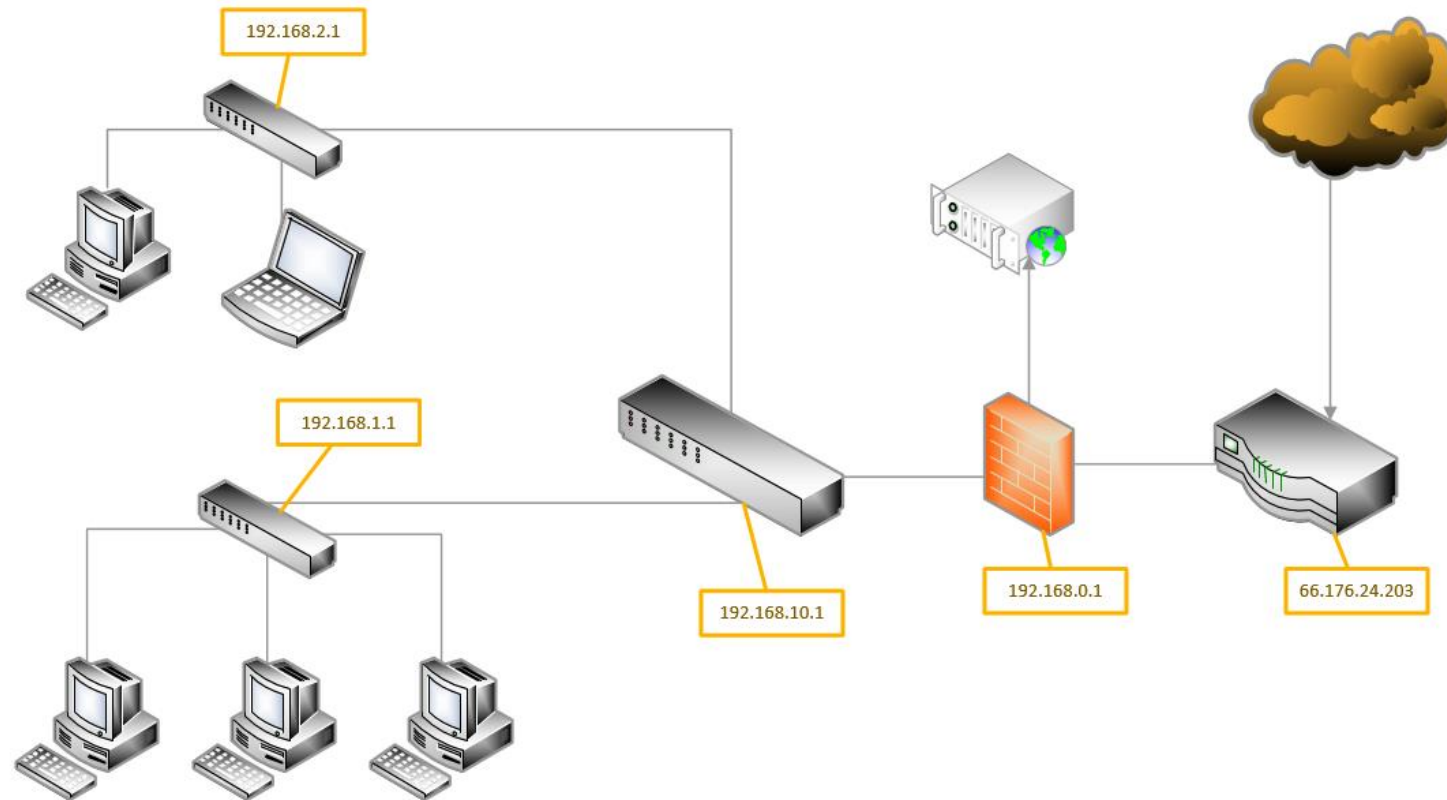
Firewalls

- One of the key devices which need to be considered
- Next generation firewalls often combine the deny/allow ruleset with IDS or IPS, as well as controlling network access to applications
- Creates a significant source of evidence that can be leveraged during an incident
- Acquiring evidence from firewalls is largely dependent on the manufacturer and the specific model that is used

Firewalls (cont.)

- Key evidence points:
 - Connection log: The connection log provides the source and destination IP addresses and protocols of connections between internal and external systems. This is critical to determining whether any internal systems may have contacted an adversary-controlled system or are possibly being controlled. In addition to allowed connections, the logs may also provide an insight into connections that were denied.
 - Remote access logs: Firewalls often serve as the Virtual Private Network (VPN) concentrator for remote access. If a remote user becomes infected via malware, they can introduce that infection into the internal network through the VPN. Remote access logs will show systems that are connected and what time they connected.

Key Network Devices (cont.)



Network Forensics Overview

- Network forensics
 - Systematic tracking of incoming and outgoing traffic
 - To ascertain how an attack was carried out or how an event occurred on a network
- Intruders leave trail behind
- Determine the cause of the abnormal traffic
 - Internal bug
 - Attackers

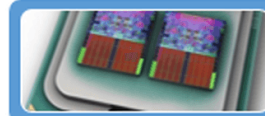
Performing Live Acquisitions

- Live acquisitions are especially useful when you're dealing with active network intrusions or attacks
- Live acquisitions done before taking a system offline are also becoming a necessity
 - Because attacks might leave footprints only in running processes or RAM
- Live acquisitions don't follow typical forensics procedures
- Order of volatility (OOV)
 - How long a piece of information lasts on a system

Order of Volatility

- Volatility is used to describe how data on a host system is maintained after changes such as log-offs or power shutdowns
- Volatile data can be data in the CPU, routing table, or ARP cache. One of the most critical pieces of volatile evidence is the memory currently running on the system
- When investigating incidents such as malware infections, the memory in a live system is of critical importance
- Non-volatile data is the data that is stored on a hard drive and will usually persist after shutting down
- Important to prioritise collection of volatile data first!

Order of Volatility (cont.)



Cache



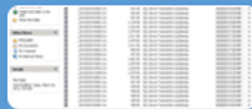
RAM



Paging File



HDD



Logs stored on remote systems



Archive Media



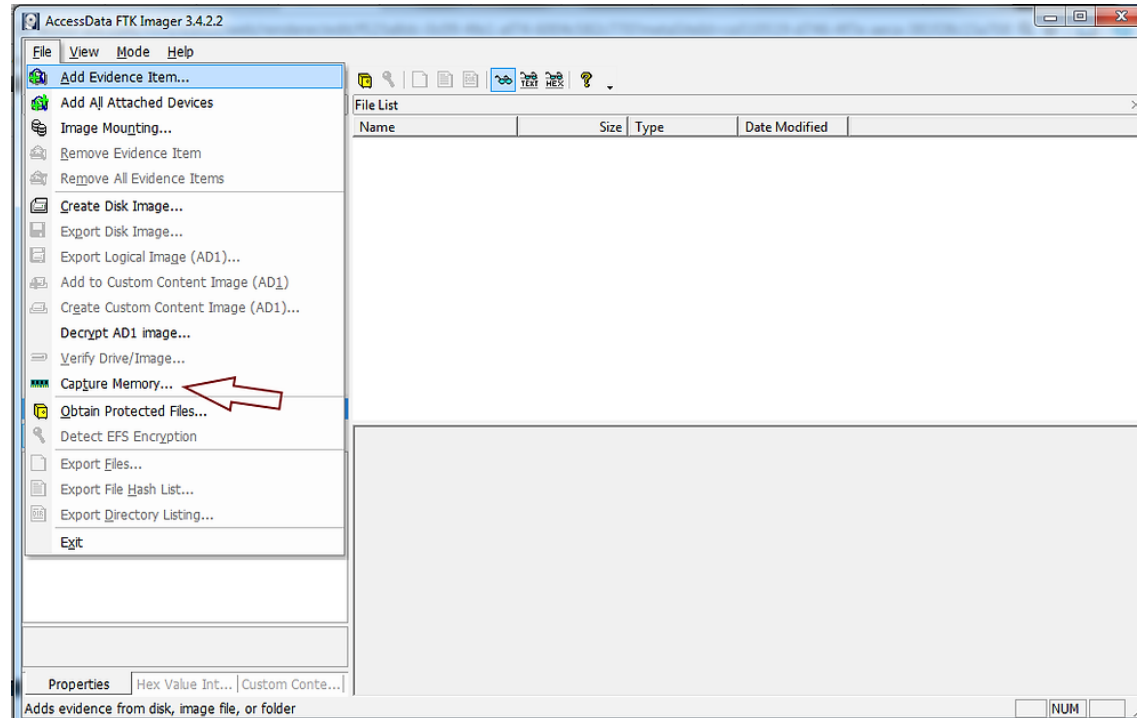
Performing Live Acquisitions (cont.)

- Steps
 - Create or download a bootable forensic CD
 - Make sure you keep a log of all your actions
 - A network drive is ideal as a place to send the information you collect
 - Copy the physical memory (RAM)
 - The next step varies, depending on the incident you're investigating
 - Be sure to get a forensic hash value of all files you recover during the live acquisition

Performing a Live Acquisition in Windows

- Several tools are available to capture the RAM.
 - Mantech Memory DD
 - Win32dd
 - winen.exe from Guidance Software
 - BackTrack 3
 - AccessData FTK Imager

Performing a Live Acquisition in Windows



Developing Standard Procedures for Network Forensics

- Long, tedious process
- Standard procedure
 - Always use a standard installation image for systems on a network
 - Close any way in after an attack
 - Attempt to retrieve all volatile data
 - Acquire all compromised drives
 - Compare files on the forensic image to the original installation image

Developing Standard Procedures for Network Forensics

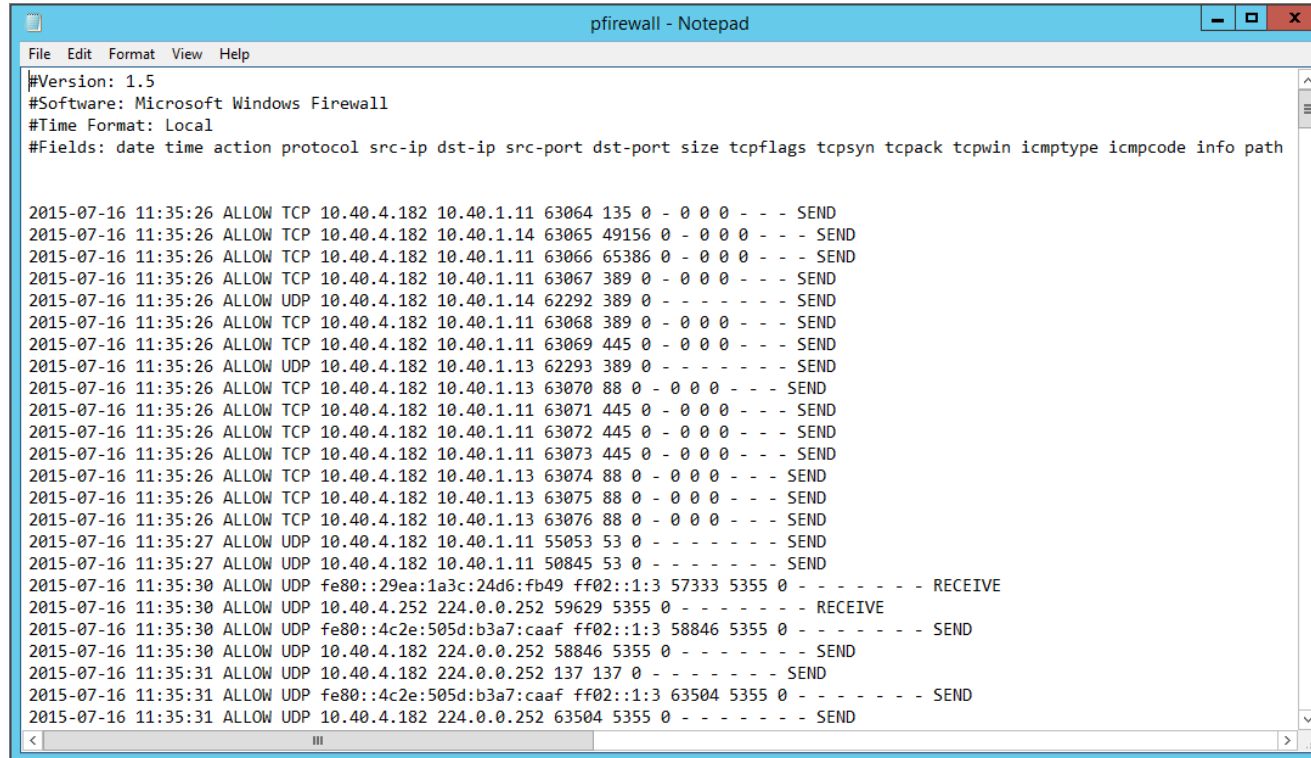
- Computer forensics
 - Work from the image to find what has changed
- Network forensics
 - Restore drives to understand attack
- Work on an isolated system
 - Prevents malware from affecting other systems

Reviewing Network Logs

- Record ingoing and outgoing traffic
 - Network servers
 - Routers
 - Firewalls
- Tcpdump tool for examining network traffic
 - Can generate top 10 lists
 - Can identify patterns
- Attacks might include other companies
 - Do not reveal information discovered about other companies

Reviewing Network Logs

The following highlights information found in firewall logs:

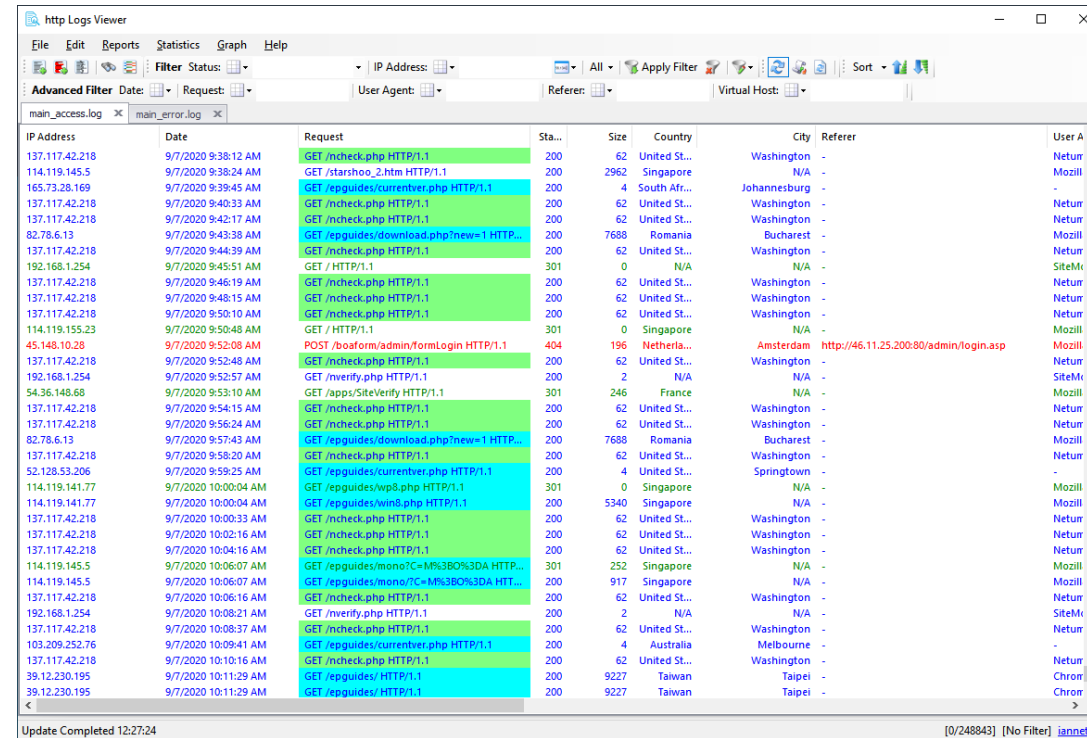


```
pfirewall - Notepad
File Edit Format View Help
#Version: 1.5
#Software: Microsoft Windows Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack tcpwin icmptype icmpcode info path

2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63064 135 0 - 0 0 0 - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.14 63065 49156 0 - 0 0 0 - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63066 65386 0 - 0 0 0 - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63067 389 0 - 0 0 0 - - SEND
2015-07-16 11:35:26 ALLOW UDP 10.40.4.182 10.40.1.14 62292 389 0 - - - - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63068 389 0 - 0 0 0 - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63069 445 0 - 0 0 0 - - SEND
2015-07-16 11:35:26 ALLOW UDP 10.40.4.182 10.40.1.13 62293 389 0 - - - - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.13 63070 88 0 - 0 0 0 - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63071 445 0 - 0 0 0 - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63072 445 0 - 0 0 0 - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63073 445 0 - 0 0 0 - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.13 63074 88 0 - 0 0 0 - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.13 63075 88 0 - 0 0 0 - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.13 63076 88 0 - 0 0 0 - - SEND
2015-07-16 11:35:27 ALLOW UDP 10.40.4.182 10.40.1.11 55053 53 0 - - - - - - SEND
2015-07-16 11:35:27 ALLOW UDP 10.40.4.182 10.40.1.11 50845 53 0 - - - - - - SEND
2015-07-16 11:35:30 ALLOW UDP fe80::29ea:1a3c:24d6:fb49 ff02::1:3 57333 5355 0 - - - - - - RECEIVE
2015-07-16 11:35:30 ALLOW UDP 10.40.4.252 224.0.0.252 59629 5355 0 - - - - - - RECEIVE
2015-07-16 11:35:30 ALLOW UDP fe80::4c2e:505d:b3a7:caaf ff02::1:3 58846 5355 0 - - - - - - SEND
2015-07-16 11:35:30 ALLOW UDP 10.40.4.182 224.0.0.252 58846 5355 0 - - - - - - SEND
2015-07-16 11:35:31 ALLOW UDP 10.40.4.182 224.0.0.252 137 137 0 - - - - - - SEND
2015-07-16 11:35:31 ALLOW UDP fe80::4c2e:505d:b3a7:caaf ff02::1:3 63504 5355 0 - - - - - - SEND
2015-07-16 11:35:31 ALLOW UDP 10.40.4.182 224.0.0.252 63504 5355 0 - - - - - - SEND
```

Reviewing Network Logs

Additionally, logs can be retrieved from web servers, which is shown below:



The screenshot shows the 'http Logs Viewer' application window. It has a menu bar (File, Edit, Reports, Statistics, Graph, Help) and a toolbar with various icons. Below the toolbar is an 'Advanced Filter' section with fields for Date, Request, User Agent, Referer, and Virtual Host. The main area displays a table of log entries. The table has columns: IP Address, Date, Request, Sta... (Status), Size, Country, City, Referrer, and User A... (User Agent). The logs are sorted by date, showing entries from 9/7/2020 9:38:12 AM to 9/7/2020 10:11:29 AM. The requests are primarily GET requests to various endpoints like /ncheck.php, /starshoo_2.htm, /epguides/currentver.php, /epguides/download.php, and /boaform/admin/formLogin. The status codes are mostly 200, with one 404. The countries listed include United States, Singapore, South Africa, Romania, Netherlands, France, and Australia. The cities listed include Washington, Johannesburg, Bucharest, Amsterdam, and Melbourne. The user agents include Mozilla, Netur, SiteMi, and Chrome.

IP Address	Date	Request	Sta...	Size	Country	City	Referrer	User A...
137.117.42.218	9/7/2020 9:38:12 AM	GET /ncheck.php HTTP/1.1	200	62	United St...	Washington	-	Netur
114.119.145.5	9/7/2020 9:38:24 AM	GET /starshoo_2.htm HTTP/1.1	200	2962	Singapore	N/A	-	Mozill
165.73.28.169	9/7/2020 9:39:45 AM	GET /epguides/currentver.php HTTP/1.1	200	4	South Afr...	Johannesburg	-	-
137.117.42.218	9/7/2020 9:40:33 AM	GET /ncheck.php HTTP/1.1	200	62	United St...	Washington	-	Netur
137.117.42.218	9/7/2020 9:42:17 AM	GET /ncheck.php HTTP/1.1	200	62	United St...	Washington	-	Netur
82.78.6.13	9/7/2020 9:43:38 AM	GET /epguides/download.php?new=1 HTTP...	200	7688	Romania	Bucharest	-	Mozill
137.117.42.218	9/7/2020 9:44:39 AM	GET /ncheck.php HTTP/1.1	200	62	United St...	Washington	-	Netur
192.168.1.254	9/7/2020 9:45:51 AM	GET / HTTP/1.1	301	0	N/A	N/A	-	SiteMi
137.117.42.218	9/7/2020 9:46:19 AM	GET /ncheck.php HTTP/1.1	200	62	United St...	Washington	-	Netur
137.117.42.218	9/7/2020 9:48:15 AM	GET /ncheck.php HTTP/1.1	200	62	United St...	Washington	-	Netur
137.117.42.218	9/7/2020 9:50:10 AM	GET /ncheck.php HTTP/1.1	200	62	United St...	Washington	-	Netur
114.119.155.23	9/7/2020 9:50:48 AM	GET / HTTP/1.1	301	0	Singapore	N/A	-	Mozill
45.148.10.28	9/7/2020 9:52:08 AM	POST /boaform/admin/formLogin HTTP/1.1	404	196	Netherla...	Amsterdam	http://46.11.25.200:80/admin/login.asp	Mozill
137.117.42.218	9/7/2020 9:52:48 AM	GET /ncheck.php HTTP/1.1	200	62	United St...	Washington	-	Netur
192.168.1.254	9/7/2020 9:52:57 AM	GET /nverify.php HTTP/1.1	200	2	N/A	N/A	-	SiteMi
54.36.148.68	9/7/2020 9:53:10 AM	GET /apps/SiteVerify HTTP/1.1	301	246	France	N/A	-	Mozill
137.117.42.218	9/7/2020 9:54:15 AM	GET /ncheck.php HTTP/1.1	200	62	United St...	Washington	-	Netur
137.117.42.218	9/7/2020 9:56:24 AM	GET /ncheck.php HTTP/1.1	200	62	United St...	Washington	-	Netur
82.78.6.13	9/7/2020 9:57:43 AM	GET /epguides/download.php?new=1 HTTP...	200	7688	Romania	Bucharest	-	Mozill
137.117.42.218	9/7/2020 9:58:20 AM	GET /ncheck.php HTTP/1.1	200	62	United St...	Washington	-	Netur
52.128.53.206	9/7/2020 9:59:25 AM	GET /epguides/currentver.php HTTP/1.1	200	4	United St...	Springtown	-	-
114.119.141.77	9/7/2020 10:00:04 AM	GET /epguides/wp8.php HTTP/1.1	301	0	Singapore	N/A	-	Mozill
114.119.141.77	9/7/2020 10:00:04 AM	GET /epguides/wp8.php HTTP/1.1	200	5340	Singapore	N/A	-	Mozill
137.117.42.218	9/7/2020 10:00:33 AM	GET /ncheck.php HTTP/1.1	200	62	United St...	Washington	-	Netur
137.117.42.218	9/7/2020 10:02:16 AM	GET /ncheck.php HTTP/1.1	200	62	United St...	Washington	-	Netur
137.117.42.218	9/7/2020 10:04:16 AM	GET /ncheck.php HTTP/1.1	200	62	United St...	Washington	-	Netur
114.119.145.5	9/7/2020 10:06:07 AM	GET /epguides/mono?C=M%3B0%3DA HTTP...	301	252	Singapore	N/A	-	Mozill
114.119.145.5	9/7/2020 10:06:07 AM	GET /epguides/mono?C=M%3B0%3DA HTTP...	200	917	Singapore	N/A	-	Mozill
137.117.42.218	9/7/2020 10:06:16 AM	GET /ncheck.php HTTP/1.1	200	62	United St...	Washington	-	Netur
192.168.1.254	9/7/2020 10:08:21 AM	GET /nverify.php HTTP/1.1	200	2	N/A	N/A	-	SiteMi
137.117.42.218	9/7/2020 10:08:37 AM	GET /ncheck.php HTTP/1.1	200	62	United St...	Washington	-	Netur
103.209.252.76	9/7/2020 10:09:41 AM	GET /epguides/currentver.php HTTP/1.1	200	4	Australia	Melbourne	-	-
137.117.42.218	9/7/2020 10:10:16 AM	GET /ncheck.php HTTP/1.1	200	62	United St...	Washington	-	Netur
39.12.230.195	9/7/2020 10:11:29 AM	GET /epguides/ HTTP/1.1	200	9227	Taiwan	Taipei	-	Chrom
39.12.230.195	9/7/2020 10:11:29 AM	GET /epguides/ HTTP/1.1	200	9227	Taiwan	Taipei	-	Chrom

Using Network Tools

- Sysinternals
 - A collection of free tools for examining Windows products
- Examples of the Sysinternals tools:
 - RegMon shows Registry data in real time
 - Process Explorer shows what is loaded
 - Handle shows open files and processes using them
 - Filemon shows file system activity

Using Network Tools (cont.)

- Tools from PsTools suite created by Sysinternals
 - PsExec runs processes remotely
 - PsGetSid displays security identifier (SID)
 - PsKill kills process by name or ID
 - PsList lists details about a process
 - PsLoggedOn shows who's logged locally
 - PsPasswd changes account passwords
 - PsService controls and views services
 - PsShutdown shuts down and restarts PCs
 - PsSuspend suspends processes

Using Packet Sniffers

- Packet sniffers
 - Devices or software that monitor network traffic
 - Most work at layer 2 or 3 of the OSI model
- Most tools follow the PCAP format
- Some packets can be identified by examining the flags in their TCP headers
- Tools
 - Tcpdump
 - Tethereal

Reviewing Network Logs

- Tools (continued)
 - Snort
 - Tcpslice
 - Tcpreplay
 - Tcpdstat
 - Ngrep
 - Etherape
 - Netdude
 - Argus
 - Ethereal

Using Packet Sniffers (cont.)

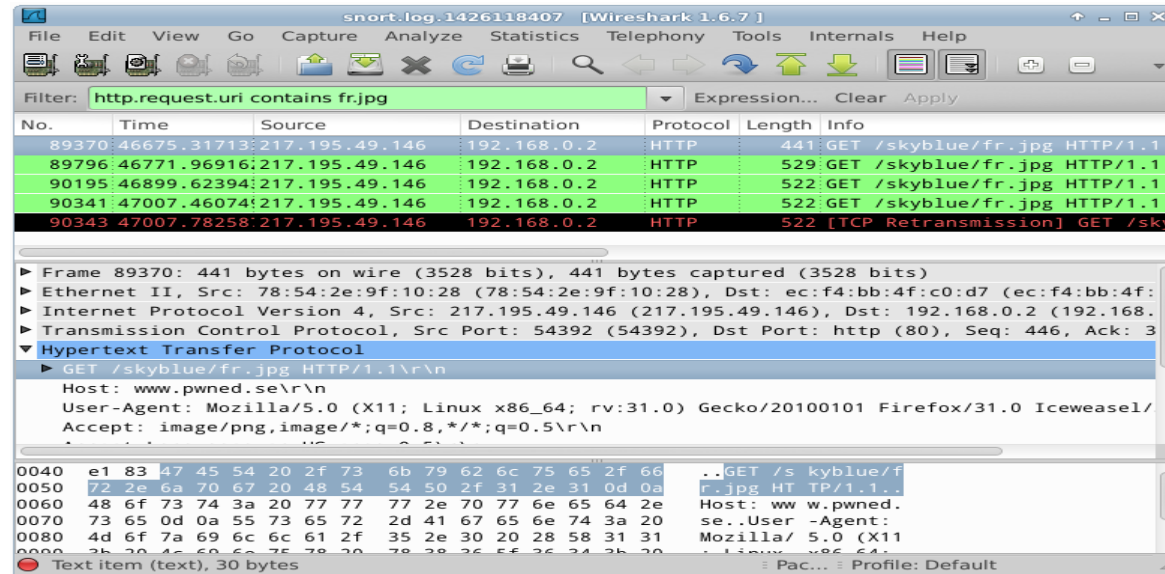
```
dedsec@kalithead: ~  
File Actions Edit View Help  
dedsec@kalithead:~$ sudo snort -vde  
Running in packet dump mode  
  
-- Initializing Snort --  
Initializing Output Plugins!  
pcap DAQ configured to passive.  
Acquiring network traffic from "eth0".  
Decoding Ethernet  
  
-- Initialization Complete --  
  
o''~  
o''~  
o''~  
o''~  
--> Snort! <*-  
Version 2.9.7.0 GRE (Build 149)  
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team  
Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.  
Copyright (C) 1998-2013 Sourcefire, Inc., et al.  
Using libpcap version 1.9.1 (with TPACKET_V3)  
Using PCRE version: 8.39 2016-06-14  
Using ZLIB version: 1.2.11  
  
Commencing packet processing (pid=5998)  
WARNING: No preprocessors configured for policy 0.  
03/05-15:26:39.026353 00:50:56:C0:00:08 -> 01:00:5E:4D:4D type:0x800 len:0x94  
192.168.52.1:12177 -> 224.77.77.77:12177 UDP TTL:1 TOS:0x0 ID:37055 IpLen:20 DgmLen:134  
Len: 106  
3C 41 53 55 53 5F 41 52 4D 4F 55 52 59 5F 43 52 <ASUS_ARMOURY_CR  
41 54 45 3E 3C 4C 41 4E 20 50 6F 72 74 3D 22 31 ATE><LAN Port="1  
32 31 37 37 22 20 43 75 73 49 44 3D 22 32 39 31 2177" CusID="291  
31 34 34 38 44 2D 41 34 42 42 2D 34 31 43 43 2D 1448D-A4BB-41CC-  
39 42 35 43 2D 43 32 42 39 32 30 37 32 30 37 30 9B5C-C2B92072070  
41 22 20 2F 3E 3C 2F 41 53 55 53 5F 41 52 4D 4F A* /></ASUS_ARMO  
55 52 59 5F 43 52 41 54 45 3E URY_CRATE>  
  
*****  
  
WARNING: No preprocessors configured for policy 0.  
03/05-15:26:39.043101 00:50:56:C0:00:08 -> 01:00:5E:4D:4D type:0x800 len:0x94  
192.168.52.1:12177 -> 224.77.77.77:12177 UDP TTL:1 TOS:0x0 ID:37056 IpLen:20 DgmLen:134  
Len: 106  
3C 41 53 55 53 5F 41 52 4D 4F 55 52 59 5F 43 52 <ASUS_ARMOURY_CR  
41 54 45 3E 3C 4C 41 4E 20 50 6F 72 74 3D 22 31 ATE><LAN Port="1  
32 31 37 37 22 20 43 75 73 49 44 3D 22 32 39 31 2177" CusID="291  
31 34 34 38 44 2D 41 34 42 42 2D 34 31 43 43 2D 1448D-A4BB-41CC-  
39 42 35 43 2D 43 32 42 39 32 30 37 32 30 37 30 9B5C-C2B92072070  
41 22 20 2F 3E 3C 2F 41 53 55 53 5F 41 52 4D 4F A* /></ASUS_ARMO  
55 52 59 5F 43 52 41 54 45 3E URY_CRATE>  
  
*****
```

Network Forensics Tools

- Wireshark is a Unix or Windows packet capture and analysis tool.
- Is a GUI-based tool and has a number of not only packet capture, but also analysis features.
- The tool is only supported on Windows or macOS

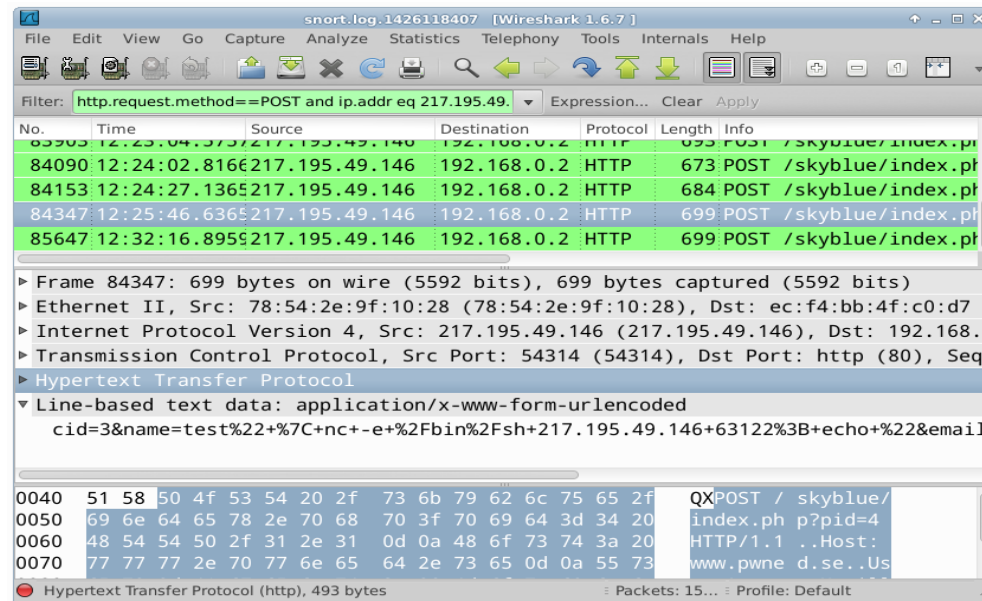
Network Forensics Tools (cont.)

- Finding the IP address used by the attackers can be found through using Wireshark



Network Forensics Tools (cont.)

- Additionally Wireshark can be used to find and filter for HTTP POST requests



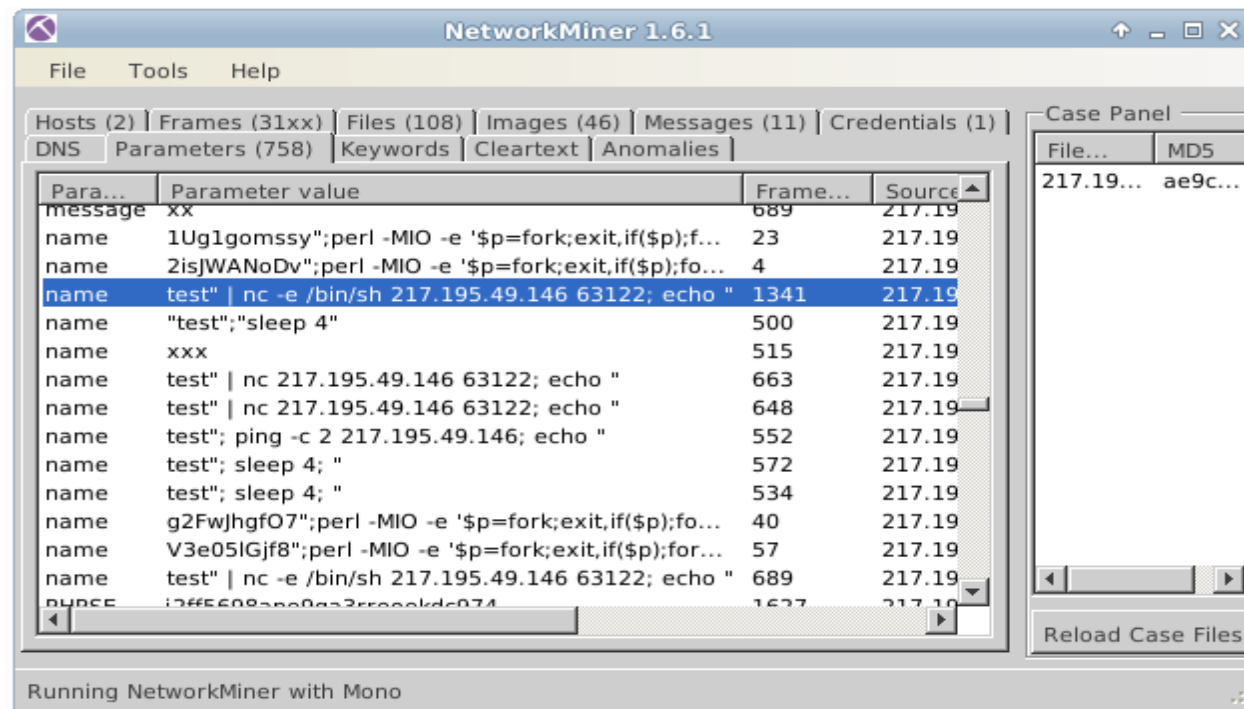
Network Forensics Tools (cont.)

- Wireshark can be used to find individual packets using its 'Find Packet' tool
- Can find By:
 - Display Filter
 - Hex value
 - **String**
- Search in (only for String search):
 - Packet list
 - Packet details
 - **Packet bytes** (this is usually what you want)



Network Forensics Tools (cont.)

- Another application which can be used is NetworkMiner
- Here, it is used to filter specifically via the 'name' parameter



Security Operations Center (SOC)

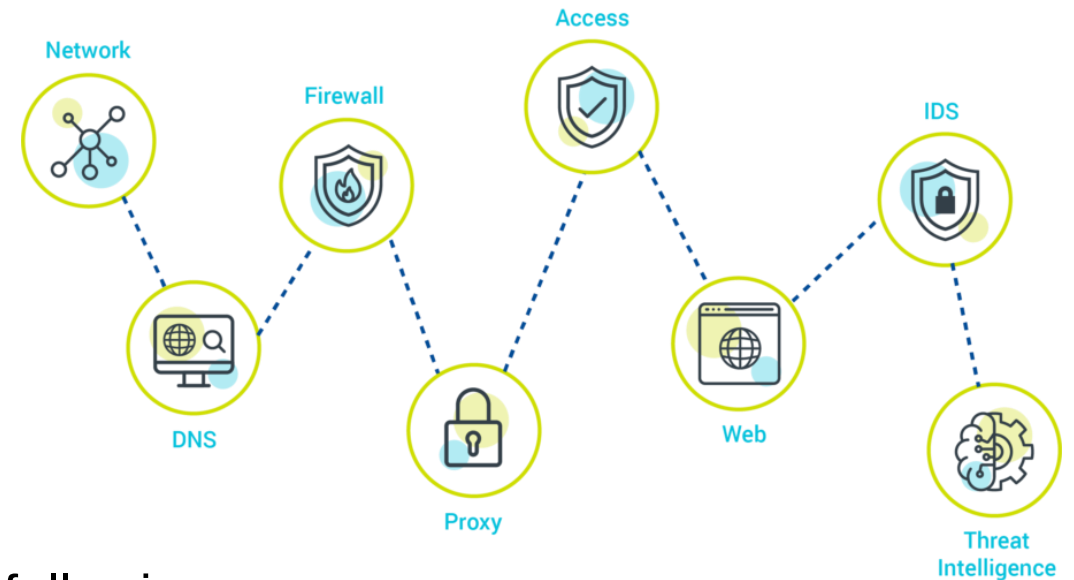
- Is a team dedicated to securing an enterprise
- Three main components to an SOC:
 - The people (analysts, architects, managers, and engineers)
 - The technologies and tools used in day-to-day operations
 - The frameworks and methodologies the team puts into practice
- The chief objective of the security operations centre is to detect, investigate, triage, and respond to real-time and historical threats to reduce cyber risk across the organization
- The key steps for an SOC are laid out below:



Security Operations Center (SOC)

- The key issues SOC investigations and forensics face are:

- Advanced Threat Actors
- Lack of Visibility
- Time-intensive Analysis
- Alert Fatigue



- The key evidence to gather can come from the following sources:

Security Operations Center (SOC)

- The following is an example of a SOC



Summary

1. Overview of Network Forensics
2. Fundamentals of Networking
3. Approach to Network Forensics
4. Examining Network traffic to identify abnormal traffic
5. Understand Network Forensics Tools
6. Order of Volatility
7. Live data acquisition and examination



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Any Questions?

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk