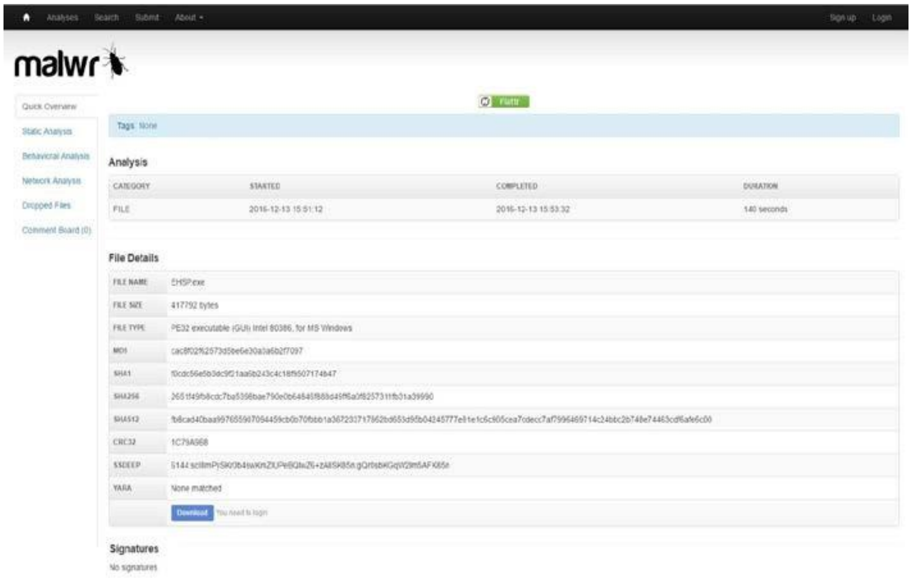
1.0 Endpoint Threat Analysis and Computer Forensics

Q. 1.1 Interpret the output report of a malware analysis tool such as AMP Threat Grid and Cuckoo Sandbox

A. Cuckoo Sandbox = Chapter 8 slide 12-14,



Tags: None

Analysis

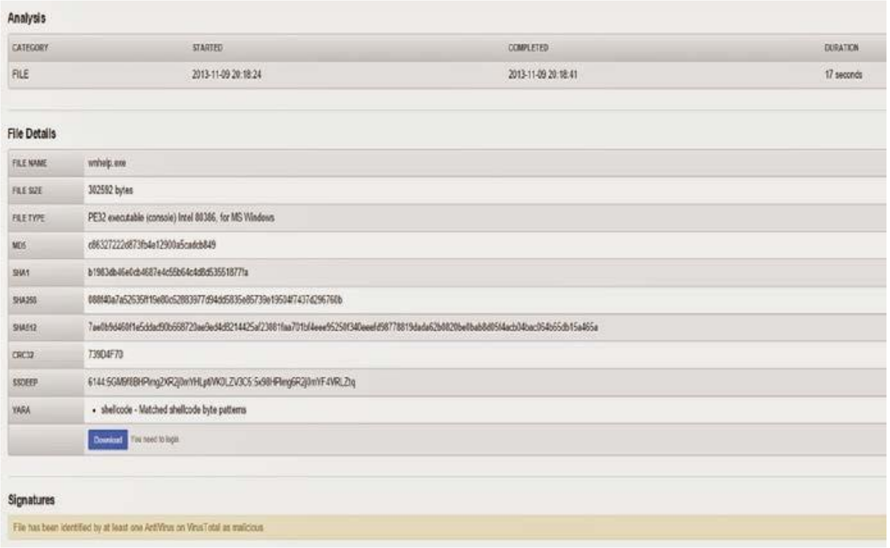
CATEGORY	STARTED	COMPLETED	DURATION
FILE	2016-12-13 15:51:12	2016-12-13 15:53:32	140 seconds

File Details

FILE NAME	EHSP.exe
FILE SIZE	417792 bytes
FILE TYPE	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	cac8f02f62573d5be6e30a3a6b2f7097
SHA1	f0cdc56e5b3dc9f21aa6b243c4c18f9507174847
SHA256	2651f49fb8cdc7ba5398bae790e0b64845f883d49f6a0f825731ffb31a39990
SHA512	fb8cad40baa997655907054459cb0b70fbbb1a367233717862bd653d95b04245777e81e1c6c905cea7cdecc7af7996469714c24bbc2b748e74463cdf6afe6c00
CRC32	1C79A968
SSDEEP	6144:scl8mPySK0b4swKmZtUPe8QtwZ6+zA8SK85n.gQrtsb#GqW29m5AFK65r
YARA	None matched
	Download You need to login

Signatures

No signatures



Analysis

CATEGORY	STARTED	COMPLETED	DURATION
FILE	2013-11-09 20:18:24	2013-11-09 20:18:41	17 seconds

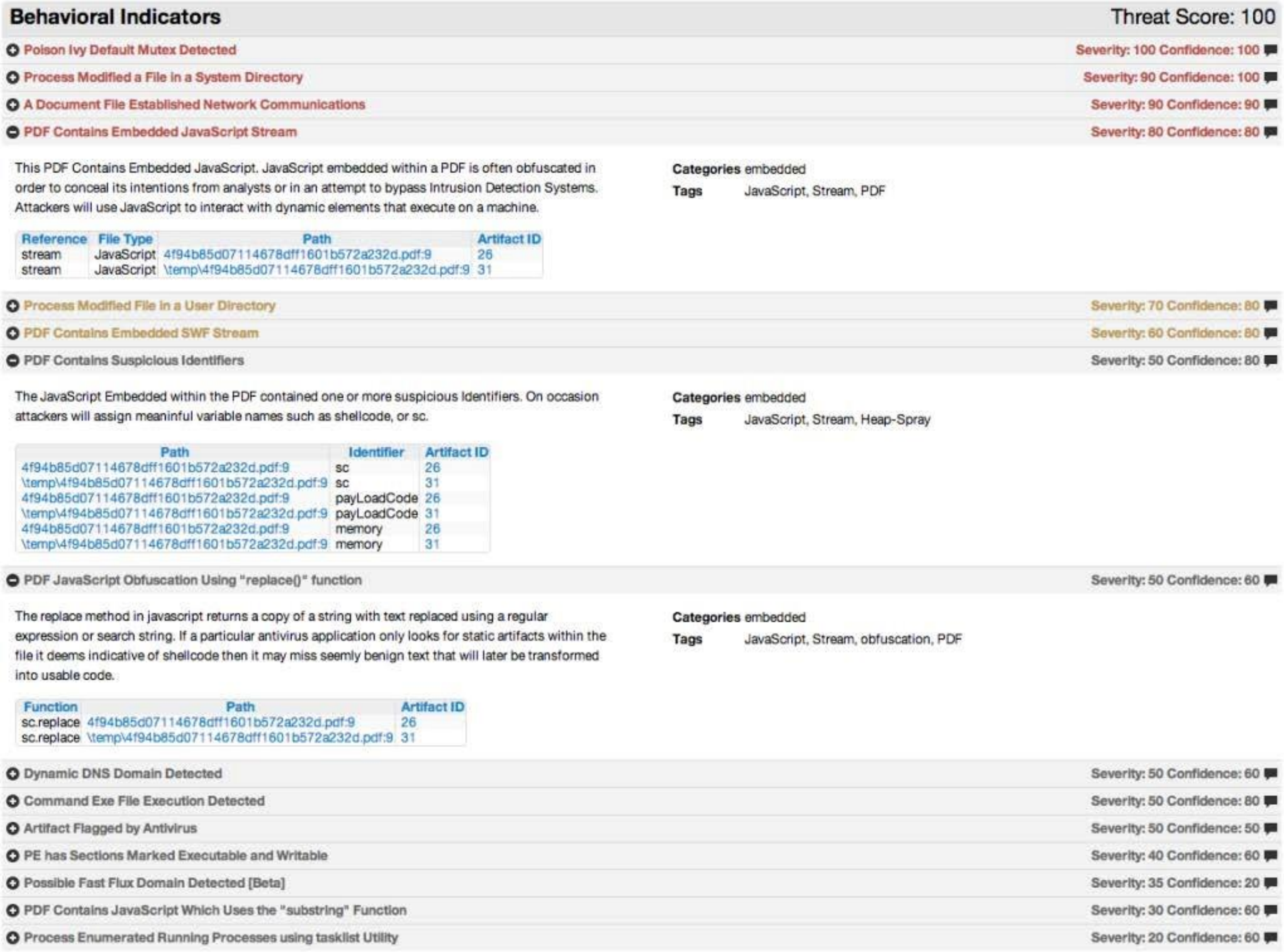
File Details

FILE NAME	wmhelp.exe
FILE SIZE	302592 bytes
FILE TYPE	PE32 executable (console) Intel 80386, for MS Windows
MD5	c86327222d873fb4e12900a5cadcb849
SHA1	b1983db46e0cb4687e4c55b64c4d8d53551877fa
SHA256	088f40a7a52635ff19e80c52883977d94dd5835e85739e19504f7437d296760b
SHA512	7ae0b9d460f1e5ddad90b668723ae9ed4d8214425af23881faa701bf4eee95250f340eeefd58778819dada62b8020be8bab8d05f4acb04bac064b65db15a465a
CRC32	739D4F70
SSDEEP	6144:5GM9f8BHPlng2XR2j0mYHLpWK0LZV3C5:5x98HPlng6R2j0mYF4VRLZtq
YARA	• shellcode - Matched shellcode byte patterns
	You need to login

Signatures

File has been identified by at least one AntiVirus on VirusTotal as malicious

AMP Threat Grid = Is a Cisco Appliance



Behavioral Indicators Threat Score: 100

Poison Ivy Default Mutex Detected	Severity: 100 Confidence: 100
Process Modified a File in a System Directory	Severity: 90 Confidence: 100
A Document File Established Network Communications	Severity: 90 Confidence: 90
PDF Contains Embedded JavaScript Stream	Severity: 80 Confidence: 80

This PDF Contains Embedded JavaScript. JavaScript embedded within a PDF is often obfuscated in order to conceal its intentions from analysts or in an attempt to bypass Intrusion Detection Systems. Attackers will use JavaScript to interact with dynamic elements that execute on a machine.

Categories embedded
Tags JavaScript, Stream, PDF

Reference	File Type	Path	Artifact ID
stream	JavaScript	4f94b85d07114678dff1601b572a232d.pdf:9	26
stream	JavaScript	\temp\4f94b85d07114678dff1601b572a232d.pdf:9	31

Process Modified File in a User Directory	Severity: 70 Confidence: 80
PDF Contains Embedded SWF Stream	Severity: 60 Confidence: 80
PDF Contains Suspicious Identifiers	Severity: 50 Confidence: 80

The JavaScript Embedded within the PDF contained one or more suspicious Identifiers. On occasion attackers will assign meaninful variable names such as shellcode, or sc.

Categories embedded
Tags JavaScript, Stream, Heap-Spray

Path	Identifier	Artifact ID
4f94b85d07114678dff1601b572a232d.pdf:9	sc	26
\temp\4f94b85d07114678dff1601b572a232d.pdf:9	sc	31
4f94b85d07114678dff1601b572a232d.pdf:9	payLoadCode	26
\temp\4f94b85d07114678dff1601b572a232d.pdf:9	payLoadCode	31
4f94b85d07114678dff1601b572a232d.pdf:9	memory	26
\temp\4f94b85d07114678dff1601b572a232d.pdf:9	memory	31

PDF JavaScript Obfuscation Using "replace()" function	Severity: 50 Confidence: 60

The replace method in javascript returns a copy of a string with text replaced using a regular expression or search string. If a particular antivirus application only looks for static artifacts within the file it deems indicative of shellcode then it may miss seemly benign text that will later be transformed into usable code.

Categories embedded
Tags JavaScript, Stream, obfuscation, PDF

Function	Path	Artifact ID
sc.replace	4f94b85d07114678dff1601b572a232d.pdf:9	26
sc.replace	\temp\4f94b85d07114678dff1601b572a232d.pdf:9	31

Dynamic DNS Domain Detected	Severity: 50 Confidence: 60
Command Exe File Execution Detected	Severity: 50 Confidence: 80
Artifact Flagged by Antivirus	Severity: 50 Confidence: 50
PE has Sections Marked Executable and Writable	Severity: 40 Confidence: 60
Possible Fast Flux Domain Detected [Beta]	Severity: 35 Confidence: 20
PDF Contains JavaScript Which Uses the "substring" Function	Severity: 30 Confidence: 60
Process Enumerated Running Processes using tasklist Utility	Severity: 20 Confidence: 60

1.2 Describe these terms as they are defined in the CVSS 3.0:

Q. 1.2.a Attack vector

A. Chapter 4 Section 5 – Good section to know

Hint: Great calculator visual that helps with understanding of the scoring system.
https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

Attack Vector (AV): This metric reflects the context by which vulnerability exploitation is possible. This metric value and the base score will be larger the more remote (logically, and physically) an attacker can be in order to exploit the vulnerable component.

- **Local**: Exploiting the vulnerability requires either physical access to the target or a local (shell) account on the target.
- **Adjacent**: Exploiting the vulnerability requires access to the local network of the target, and cannot be performed across an OSI Layer 3 boundary.

- **Network**: The vulnerability is exploitable from remote networks. Such a vulnerability is often termed "remotely exploitable" and can be thought of as an attack being exploitable one or more network hops away such as across Layer 3 boundaries from routers.

- **Physical:** A vulnerability exploitable with physical access requires the attacker to physically touch or manipulate the vulnerable component.

Q. 1.2.b Attack Complexity

A. Attack Complexity (AC): This metric describes the conditions beyond the attacker's control that must exist in order to exploit the vulnerability.

- **Low**: Specialized access conditions or extenuating circumstances do not exist. An attacker can expect repeatable success against the vulnerable component.

- **High**: A successful attack depends on conditions beyond the attacker's control. That is, a successful attack cannot be accomplished at will, but requires the attacker to invest in some measurable amount of effort in preparation or execution against the vulnerable component before a successful attack can be expected.

Q. 1.2.c Privileges required

A. Privileges Required (PR): This metric describes the level of privileges an attacker must possess before successfully exploiting the vulnerability.

- **None**: The attacker is unauthorized before attack, and therefore does not require any access to settings or files to carry out an attack.

- **Low**: The attacker is authorized with privileges that provide basic user capabilities that could normally affect only settings and files that are owned by a user. Alternatively, an attacker with low privileges may have the ability to cause an impact only to non-sensitive resources only.

- **High**: The attacker is authorized with privileges that provide significant (e.g. administrative) control over the vulnerable component that could affect component-wide settings and files.

Q. 1.2.d User interaction

A. User Interaction (UI): Measures the impact on confidentiality of a successful exploit of the vulnerability on the target system.

- **None**: The vulnerable system can be exploited without interaction from any user.

- **Required**: Successful exploitation of this vulnerability requires a user to take some action before the vulnerability can be exploited.

Q. 1.2.e Scope

A. Scope (S): An important property that is captured by CVSS v3.0 is the ability for a vulnerability in one software component to impact resources beyond its means, or privileges. This consequence is represented by the metric Authorization Scope, or simply Scope.

- **Unchanged:** An exploited vulnerability can only affect resources that are managed by the same authority. In this case, the vulnerable component and the impacted component are the same.

- **Changed:** An exploited vulnerability can affect resources beyond the authorization privileges that are intended by the vulnerable component. In this case, the vulnerable component and the impacted component are different.

1.3 Describe these terms as they are defined in the CVSS 3.0

Q. 1.3.a Confidentiality

A. Confidentiality Impact (C): This metric measures the impact to the confidentiality of the information resources that are managed by a software component due to a successfully exploited vulnerability. Confidentiality refers to limiting information access and disclosure to only authorized users, preventing access by, or disclosure to, unauthorized ones.

- **None**: There is no loss of confidentiality within the impacted component.
- **Low**: There is some loss of confidentiality. Access to some restricted information is obtained, but the attacker control over what information is obtained, or the amount or kind of loss is constrained. The information disclosure does not cause a direct, serious loss to the impacted component.
- **High**: There is total loss of confidentiality, resulting in all resources within the impacted component being divulged to the attacker. Alternatively, access to only some restricted information is obtained, but the disclosed information presents a direct, serious impact.

Q. 1.3.b Integrity

A. Integrity Impact (I): This metric measures the impact to integrity of a successfully exploited vulnerability. Integrity refers to the trustworthiness and veracity of information.

None: There is no loss of integrity within the impacted component.

Low: Modification of data is possible, but the attacker does not control the consequence of a modification, or the amount of modification is constrained. The data modification does not have a direct, serious impact on the impacted component.

High: There is a total loss of integrity, or a complete loss of protection. For example, the attacker is able to modify any/all files that are protected by the impacted component. Alternatively, only some files can be modified, but malicious modification would present a direct, serious consequence to the impacted component.

Q. 1.3.c Availability

A. Availability Impact (A): This metric measures the impact to the availability of the impacted component resulting from a successfully exploited vulnerability. While the Confidentiality and Integrity impact metrics apply to the loss of confidentiality or integrity of data such as information and files used by the impacted component, this metric refers to the loss of availability of the impacted component itself, such as a networked service such as web, database, and email. Because availability refers to the accessibility of information resources, attacks that consume network bandwidth, processor cycles, or disk space all impact the availability of an impacted component.

None: There is no impact to availability within the impacted component.

Low: There is reduced performance or interruptions in resource availability. Even if repeated exploitation of the vulnerability is possible, the attacker does not have the ability to completely deny service to legitimate users. The resources in the impacted component are either partially available all the time, or fully available only some of the time, but overall there is no direct, serious consequence to the impacted component.

High: There is total loss of availability, resulting in the attacker being able to fully deny access to resources in the impacted component; this loss is either sustained (while the attacker continues to deliver the attack) or persistent (the condition persists even after the attack has completed). Alternatively, the attacker has the ability to deny some availability, but the loss of availability presents a direct, serious consequence to the impacted component such as the attacker cannot disrupt existing connections, but can prevent new connections; the attacker can repeatedly exploit a vulnerability that, in each instance of a successful attack, leaks an only small amount of memory, but after repeated exploitation causes a service to become completely unavailable.

Q. 1.4 Define these items as they pertain to the Microsoft Windows file system (Chapter 8 Slide 7, 8)
1.4.a FAT32 = File Allocation Table 32, The purpose of FAT32 was to overcome the limitations of FAT16 and add support for larger media. The major enhancements introduced by FAT32 included support for much larger volumes, better performance and more flexibility and robustness. FAT32 increases standard maximum volume size from 2GB limit to 2TB.

1.4.b NTFS = New Technology File System (NTFS) is most common file system for Windows, Supports large files and partitions, Supports disk quotas, Security, Encryption, Access control via permissions

1.4.c Alternative Data Streams = Alternate Data Streams (ADS), Files are stored as attributes, One attribute is $DATA which represents the actual data of the file, NTFS allows additional data to be part of the $DATA attribute that applications can use, ADS data is not displayed by DIR command alone, Must use /r option, ADS can be used to hide malicious code in files

1.4.d MACE = NTFS keeps track of lots of time stamps. Each file has a time stamp for 'Create', 'Modify', 'Access', and 'Entry Modified'. The latter refers to the time when the MFT entry itself was modified. These four values are commonly abbreviated as the 'MACE' values. (Modified, Accessed, Created, Entry) = MACE

1.4.e EFI = Extensible Firmware Interface, (EFI system partition =ESP) When a computer is booted, EFI firmware loads files stored on the ESP to start installed operating systems and various utilities. An ESP needs to be formatted with a file system whose specification is based on the FAT file system and maintained as part of the UEFI specification; therefore, the file system specification is independent from the original FAT specification
1.4.f Free space = available space on a disk drive
1.4.g Timestamps on a file system = A timestamp is the time at which an event is recorded by a computer, not the time of the event itself. This data is usually presented in a consistent format, allowing for easy comparison of two different records and tracking progress over time; The sequential numbering

of events is sometimes called timestamping. Timestamps are typically used for logging events or in a sequence of events

Q. 1.5 Define these terms as they pertain to the Linux file system
A. 1.5.a EXT4 = A journaling filesystem for Linux is ext4. Ext4 is designed to accommodate terabyte (1024 gigabytes) HDD capacities, and it features support for storage up to 1024 petabytes (1024 terabytes) per volume.
A. 1.5.b Journaling = A *journaling filesystem* is a *filesystem* that maintains a special file called a *journal* that is used to repair any inconsistencies that occur as the result of an improper shutdown of a computer. Such shutdowns are usually due to an interruption of the power supply or to a software problem that cannot be resolved without a rebooting.
A. 1.5.c MBR = The *master boot record* (MBR) is a small program that is executed when a computer is *booting* (i.e., starting up) in order to find the operating system and load it into memory. The BIOS will search for an MBR in any of several devices or media, such as the hard disk, floppy, CDROM and USB. **A.** 1.5.d Swap file system = Linux divides its physical RAM (random access memory) into chucks of memory called pages. Swapping is the process whereby a page of memory is copied to the preconfigured space on the hard disk, called swap space, to free up that page of memory. The combined sizes of the physical memory and the swap space is the amount of virtual memory available.

A **swap file** is a file on a hard drive that is used as a temporary location to store information not being used by the computer RAM. By using a swap file, a computer can use more memory than what is physically installed in the computer.

A. 1.5.e MAC = In (**MAC**) refers to a type of access control by which the operating system computer security, **mandatory access control** constrains the ability of a *subject* or *initiator* to access or generally perform some sort of operation on an *object* or *target*. In practice, a subject is usually a process or thread; objects are constructs such as files, directories, TCP/UDP ports, shared memory segments, IO devices, etc. Subjects and objects each have a set of security attributes. Whenever a subject attempts to access an object, an authorization rule enforced by the operating system kernel examines these security attributes and decides whether the access can take place. Any operation by any subject on any object is tested against the set of authorization rules (aka *policy*) to determine if the operation is allowed. A database management system, in its access control mechanism, can also apply mandatory access control; in this case, the objects are tables, views, procedures, etc.

Q. 1.6 Compare and contrast three types of evidence
A. 1.6.a Best evidence = Best evidence is different in the digital era. Often the original document is created on a computer and stored in a binary file. While the binary file may be the most accurate original, it is gibberish to most people. Precedent has been set to submit printouts, video, and audio, that is generated from files that convey the intent of the original, in modern courts of law as best evidence.
A. 1.6.b Corroborative evidence = Corroborating evidence is evidence that supports an assertion that is supported by previously obtained evidence. The existence of corroborating evidence increases the level of confidence in the assertion.

1.6.c Indirect evidence = **Circumstantial evidence:** Requires an inference linking the evidence to the conclusion drawn from the evidence and sometimes called indirect evidence.

Q. 1.7 Compare and contrast two types of image

A. 1.7.a Altered disk image = The most common technique used to demonstrate that data has not been altered is that of "hashing". The value of creating such a hash derives from the fact that changing just the smallest element of the data source will result in a completely different hash being generated by the same algorithm, thus showing that the original data has been altered in some way. It is good forensic practice therefore to create a "hash" of the data which has been secured as early as possible during an investigation so that evidence presented at a later stage can be recognized as being derived from the data which was seized.

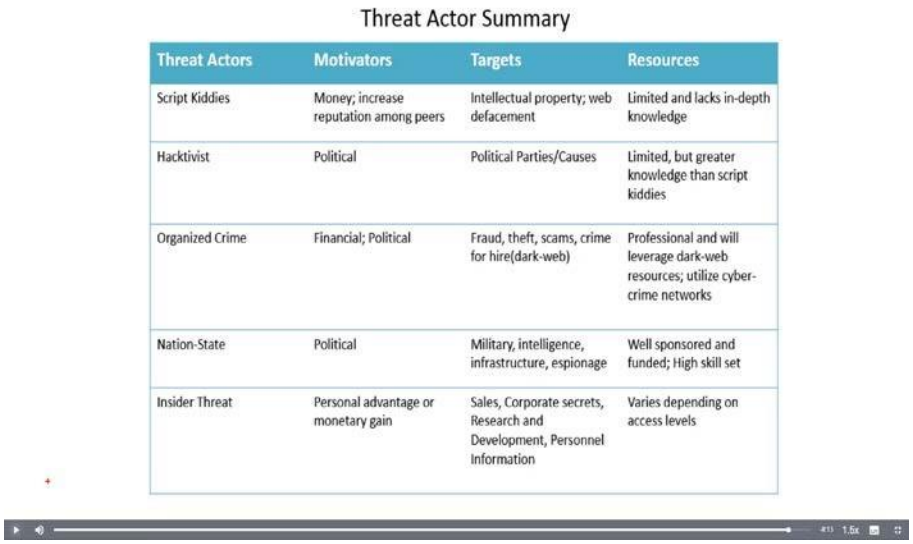
A. 1.7.b Unaltered disk image = Disk imaging – extracting unaltered bit streams from digital storage media (magnetic, optical, or solid-state) – is used for a variety of purposes. These include data rescue and recovery, full backup, cloning of drives to provision new hardware, and the creation of images that can be mounted and used as virtual drives by an operating system.

Q. 1.8 Describe the role of attribution in an investigation

A. Attribution = Assignment of a sample of questioned origin to a source of known origin to a high degree of scientific certainty, (Digital Forensics: Enough evidence to assign a source to a malware)

A. 1.8.a Assets = Assuming the analyst has obtained the network topology diagram and a list of network assets with an assignment roster, they can begin to categorize assets on the list as belonging to a particular priority such as critical, important, or sensitive. Categorizing the assets will assist the analyst with prioritizing responses to potential threats on the network. For example, an indicator of compromise to a web server located in the DMZ of the network would represent a lower priority than an IOC/(incident of compromise) to an internal Windows host system within the Accounting/Payroll department.

A. 1.8.b Threat actor = Chapter 7 slide 9:



Threat Actor Summary

Threat Actors	Motivators	Targets	Resources
Script Kiddies	Money; increase reputation among peers	Intellectual property; web defacement	Limited and lacks in-depth knowledge
Hacktivist	Political	Political Parties/Causes	Limited, but greater knowledge than script kiddies
Organized Crime	Financial; Political	Fraud, theft, scams, crime for hire(dark-web)	Professional and will leverage dark-web resources; utilize cyber-crime networks
Nation-State	Political	Military, intelligence, infrastructure, espionage	Well sponsored and funded; High skill set
Insider Threat	Personal advantage or monetary gain	Sales, Corporate secrets, Research and Development, Personnel Information	Varies depending on access levels

2.0 Network Intrusion Analysis

Q. 2.1 Interpret basic regular expressions

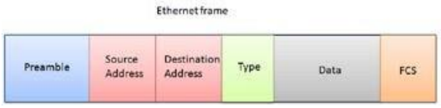
A. Practice on this website:

https://regexone.com/lesson/introduction_abcs

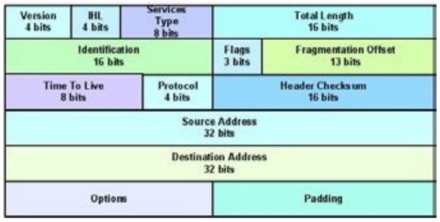
Q. 2.2 Describe the fields in these protocol headers as they relate to intrusion analysis:

A. Look at various Graphics and answer questions.

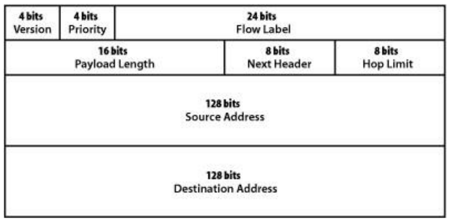
2.2.a Ethernet frame=



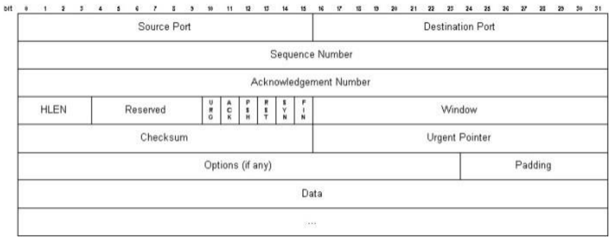
2.2.b IPv4=



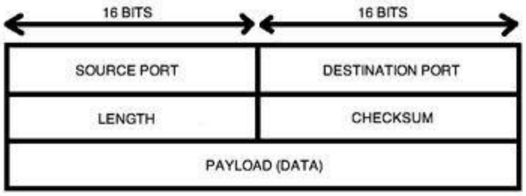
2.2.c IPv6=



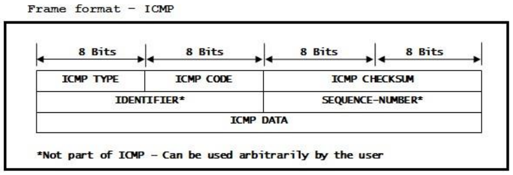
2.2.d TCP=



2.2.e UDP=



2.2.f ICMP=

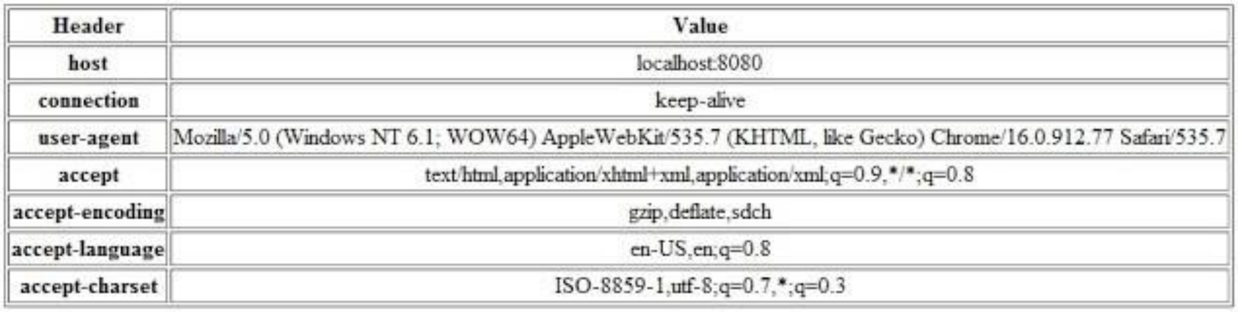


Frame format – ICMP

8 Bits	8 Bits	8 Bits	8 Bits
ICMP TYPE	ICMP CODE	ICMP CHECKSUM	
IDENTIFIER*		SEQUENCE-NUMBER*	
ICMP DATA			

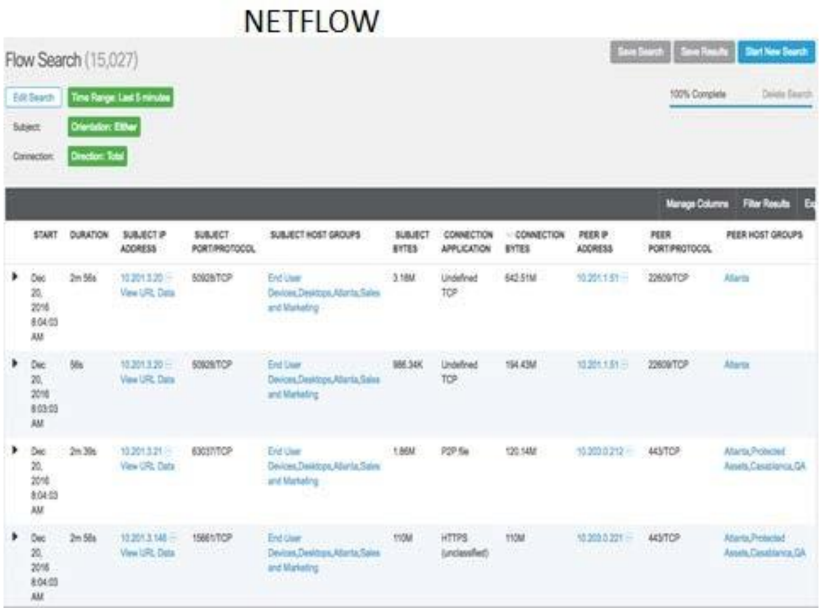
*Not part of ICMP – Can be used arbitrarily by the user

2.2.g HTTP = see below, know user agent field



Header	Value
host	localhost:8080
connection	keep-alive
user-agent	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/535.7 (KHTML, like Gecko) Chrome/16.0.912.77 Safari/535.7
accept	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
accept-encoding	gzip,deflate,sdch
accept-language	en-US,en;q=0.8
accept-charset	ISO-8859-1,utf-8;q=0.7,*;q=0.3

2.3 Identify the elements from a NetFlow v5 record from a security event



NETFLOW

Flow Search (15,027)

Time Range: Last 5 minutes

Subject: Orientation: Either

Connection: Direction: Total

	START	DURATION	SUBJECT IP ADDRESS	SUBJECT PORT/PROTOCOL	SUBJECT HOST GROUPS	SUBJECT BYTES	CONNECTION APPLICATION	CONNECTION BYTES	PEER IP ADDRESS	PEER PORT/PROTOCOL	PEER HOST GROUPS
▸	Dec 20, 2016 8:04:03 AM	2m 56s	10.201.3.20 View URL Data	50928/TCP	End User Devices,Desktops,Atlanta,Sales and Marketing	3.18M	Undefined TCP	642.51M	10.201.1.51	22609/TCP	Atlanta
▸	Dec 20, 2016 8:03:03 AM	56s	10.201.3.20 View URL Data	50928/TCP	End User Devices,Desktops,Atlanta,Sales and Marketing	986.34K	Undefined TCP	194.43M	10.201.1.51	22609/TCP	Atlanta
▸	Dec 20, 2016 8:04:03 AM	2m 39s	10.201.3.21 View URL Data	63037/TCP	End User Devices,Desktops,Atlanta,Sales and Marketing	1.86M	P2P file	120.14M	10.203.0.212	443/TCP	Atlanta,Protected Assets,Casablanca,QA
▸	Dec 20, 2016 8:04:03 AM	2m 58s	10.201.3.148 View URL Data	15661/TCP	End User Devices,Desktops,Atlanta,Sales and Marketing	110M	HTTPS (unclassified)	110M	10.203.0.221	443/TCP	Atlanta,Protected Assets,Casablanca,QA

2.4 Identify these key elements in an intrusion from a given PCAP file

2.4.a Source address

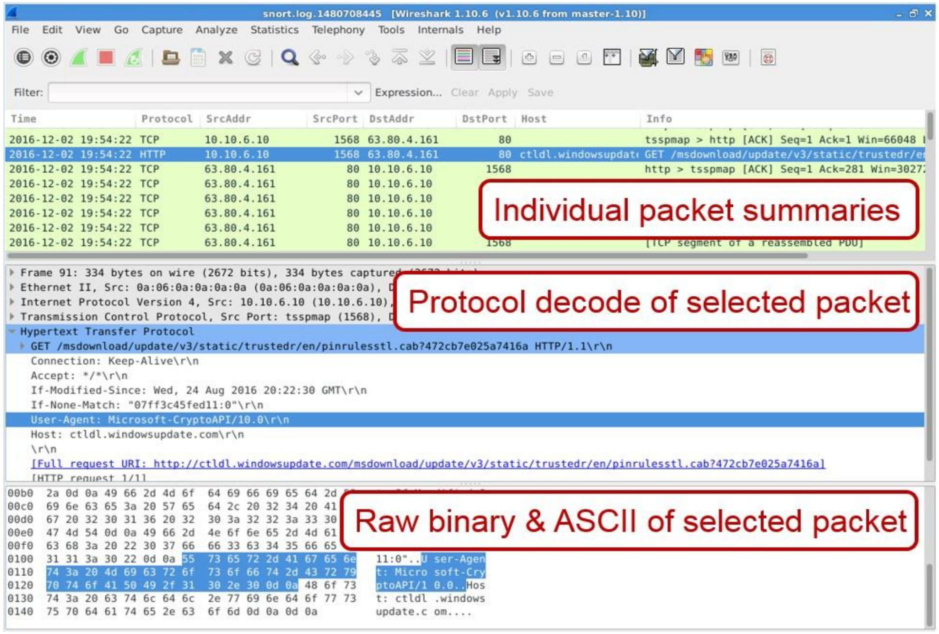
2.4.b Destination address

2.4.c Source port

2.4.d Destination port

2.4.e Protocols

2.4.f Payloads



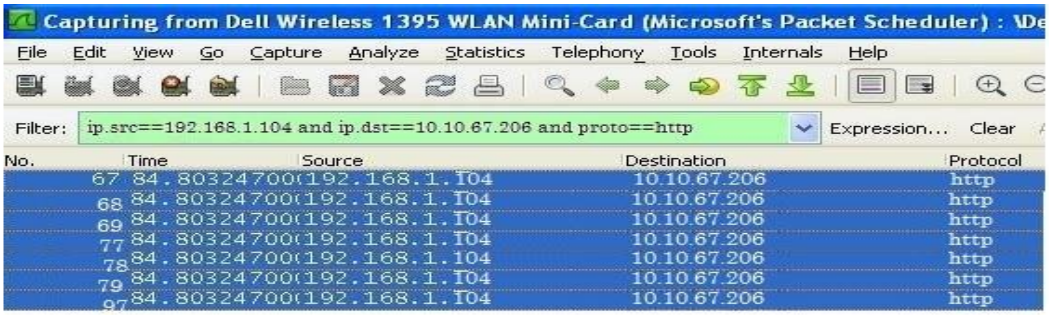
```
snort.log.1480708445  [Wireshark 1.10.6 (v1.10.6 from master-1.10)]

Filter:                                Expression...  Clear  Apply  Save

Time                 Protocol  SrcAddr      SrcPort  DstAddr      DstPort  Host                     Info
2016-12-02 19:54:22  TCP       10.10.6.10      1568  63.80.4.161       80                           tsspmap > http [ACK] Seq=1 Ack=1 Win=66048
2016-12-02 19:54:22  HTTP      10.10.6.10      1568  63.80.4.161       80  ctldl.windowsupdat       GET /msdownload/update/v3/static/trustedr/e
2016-12-02 19:54:22  TCP       63.80.4.161       80  10.10.6.10      1568                           http > tsspmap [ACK] Seq=1 Ack=281 Win=3027
2016-12-02 19:54:22  TCP       63.80.4.161       80  10.10.6.10
2016-12-02 19:54:22  TCP       63.80.4.161       80  10.10.6.10
2016-12-02 19:54:22  TCP       63.80.4.161       80  10.10.6.10
2016-12-02 19:54:22  TCP       63.80.4.161       80  10.10.6.10
2016-12-02 19:54:22  TCP       63.80.4.161       80  10.10.6.10      1568                           [TCP segment of a reassembled PDU]

▸ Frame 91: 334 bytes on wire (2672 bits), 334 bytes captured
▸ Ethernet II, Src: 0a:06:0a:0a:0a:0a (0a:06:0a:0a:0a:0a), D
▸ Internet Protocol Version 4, Src: 10.10.6.10 (10.10.6.10),
▸ Transmission Control Protocol, Src Port: tsspmap (1568), D
▾ Hypertext Transfer Protocol
  ▸ GET /msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?472cb7e025a7416a HTTP/1.1\r\n
    Connection: Keep-Alive\r\n
    Accept: */*\r\n
    If-Modified-Since: Wed, 24 Aug 2016 20:22:30 GMT\r\n
    If-None-Match: "07ff3c45fed11:0"\r\n
    User-Agent: Microsoft-CryptoAPI/10.0\r\n
    Host: ctldl.windowsupdate.com\r\n
    \r\n
    [Full request URI: http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?472cb7e025a7416a]
    [HTTP request 1/1]

00b0  2a 0d 0a 49 66 2d 4d 6f  64 69 66 69 65 64 2d
00c0  69 6e 63 65 3a 20 57 65  64 2c 20 32 34 20 41
00d0  67 20 32 30 31 36 20 32  30 3a 32 32 3a 33 30
00e0  47 4d 54 0d 0a 49 66 2d  4e 6f 6e 65 2d 4d 61
00f0  63 68 3a 20 22 30 37 66  66 33 63 34 35 66 65
0100  31 31 3a 30 22 0d 0a 55  73 65 72 2d 41 67 65 6e   11:0"..U ser-Agen
0110  74 3a 20 4d 69 63 72 6f  73 6f 66 74 2d 43 72 79   t: Micro soft-Cry
0120  70 74 6f 41 50 49 2f 31  30 2e 30 0d 0a 48 6f 73   ptoAPI/1 0.0..Hos
0130  74 3a 20 63 74 6c 64 6c  2e 77 69 6e 64 6f 77 73   t: ctldl .windows
0140  75 70 64 61 74 65 2e 63  6f 6d 0d 0a 0d 0a         update.c om....
```

Individual packet summaries

Protocol decode of selected packet

Raw binary & ASCII of selected packet

2.5 Extract files from a TCP stream when given a PCAP file and Wireshark



```
Capturing from Dell Wireless 1395 WLAN Mini-Card (Microsoft's Packet Scheduler) : \De

Filter: ip.src==192.168.1.104 and ip.dst==10.10.67.206 and proto==http    Expression...  Clear

No.  Time           Source            Destination    Protocol
 67  84.80324700(192.168.1.104        10.10.67.206   http
 68  84.80324700(192.168.1.104        10.10.67.206   http
 69  84.80324700(192.168.1.104        10.10.67.206   http
 77  84.80324700(192.168.1.104        10.10.67.206   http
 78  84.80324700(192.168.1.104        10.10.67.206   http
 79  84.80324700(192.168.1.104        10.10.67.206   http
 97  84.80324700(192.168.1.104        10.10.67.206   http
```

PCAP ANALYSIS: FILTER IN GREEN

SOURCE IP = 192.168.1.104, DESTINATION IP = 10.10.67.206, PROTOCOL = HTTP FILTER USING REGULAR EXPRESSIONS:

ip.src matches “192\.168\.1\.10[1-9]”	IP SOURCE ADDRESS IS 192.168.1.10(ANY NUMBER) \. MEANS Use the period because the (.) has other meaning with Regex [1-9] MEANS ANY NUMBER
ip.src matches “192\.168\.1\.1[246]0”	IP SOURECE ADDRESSS IS EITHER 192.168.1.120, 140, OR 160 [246] MEANS 2, 4, OR 6

What Wireshark command is used to filter/extract an ip address or name of a host? Well, there several possibilities:

Ip.src==192.168.92.103

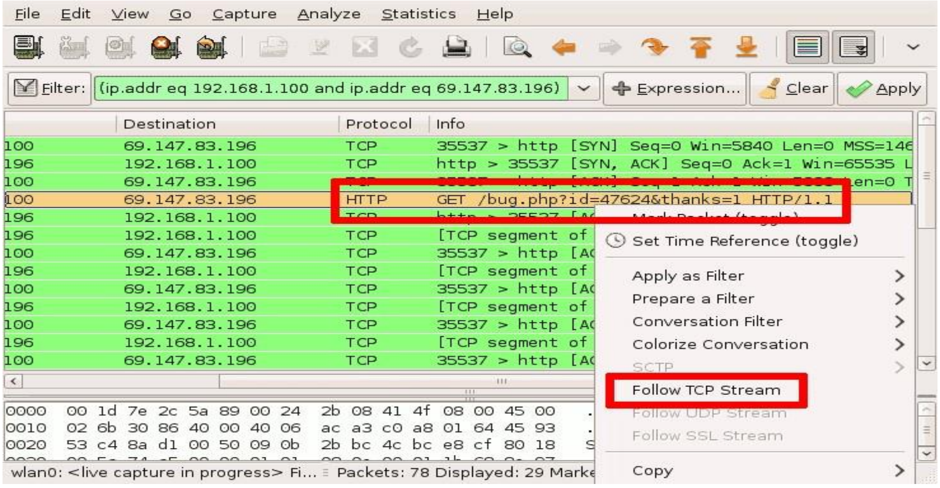
Ip.src_host==192.168.92.103

Ip.dst==192.168.92.103

Ip.addr==192.168.92.103

Ip.host==192.168.92.103

Wireshark can be used to view a Packet CAPture (PCAP) file. Use the “Follow TCP Stream” feature to follow an HTTP session. A right-click on the HTTP entry will bring up the menu with the follow the stream option.



```
Filter: (ip.addr eq 192.168.1.100 and ip.addr eq 69.147.83.196)

     Destination       Protocol  Info
100  69.147.83.196     TCP       35537 > http [SYN] Seq=0 Win=5840 Len=0 MSS=146
196  192.168.1.100     TCP       http > 35537 [SYN, ACK] Seq=0 Ack=1 Win=65535 L
100  69.147.83.196                                                    en=0 T
100  69.147.83.196     HTTP      GET /bug.php?id=47624&thanks=1 HTTP/1.1
196  192.168.1.100
196  192.168.1.100     TCP       [TCP segment of
100  69.147.83.196     TCP       35537 > http [AC
196  192.168.1.100     TCP       [TCP segment of
100  69.147.83.196     TCP       35537 > http [AC
196  192.168.1.100     TCP       [TCP segment of
100  69.147.83.196     TCP       35537 > http [AC
196  192.168.1.100     TCP       [TCP segment of
100  69.147.83.196     TCP       35537 > http [AC

0000  00 1d 7e 2c 5a 89 00 24  2b 08 41 4f 08 00 45 00   .
0010  02 6b 30 86 40 00 40 06  ac a3 c0 a8 01 64 45 93   .
0020  53 c4 8a d1 00 50 09 0b  2b bc 4c bc e8 cf 80 18   S

wlan0: <live capture in progress> Fi...  Packets: 78 Displayed: 29 Marke
```

Another example: What command do you use to extract a file from Wireshark? File > Export Object

A simple display filter can look for an exact IP source address using the equal operator. A filter of “ip.src==192.168.1.104” would show any packets that contained 192.168.1.104 as the source address.

Instead of typing every IP address from 192.168.1.101 to 192.168.1.109 into the filter, a REGEX can find them all with just one pattern. The filter would be:

```
ip.src matches “192\.168\.1\.10[1-9]”
```

While it looks complex, it is far easier than chaining multiple statements together using “or”. The “\” is used to escape the period since it is a special character interpreted literally as part of the string. The brackets denote a character class which in this case is any digit from 1 to 9. This method of filtering for a range of values can only be done using REGEX.

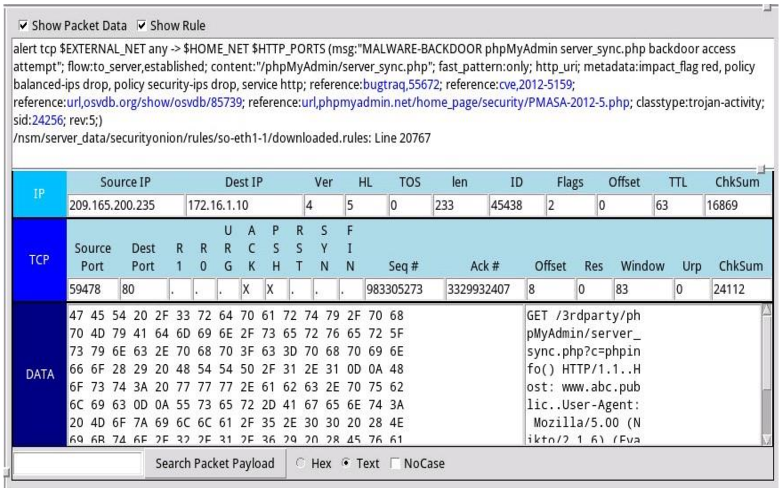
Character classes are also useful for creating lists. If the servers in this network are 192.168.1.120, 192.168.1.140, and 192.168.1.160, they could all be found with:

```
ip.src matches “192\.168\.1\.1[246]0”
```

Q. 2.6 Interpret common artifact elements from an event to identify an alert
2.6.a IP address (source / destination)
2.6.b Client and Server Port Identity
2.6.c Process (file or registry)

2.6.d System (API calls) = Powershell usage should be monitor for suspicious activity, because it is an extremely powerful command line interface. Modifying system settings and simply starting new processes is possible through Powershell, which has access to all the built-in .NET APIs and any executables that are on the system. With the right credentials, remote sessions can be opened to other computers using Powershell. A network log on from a specific user may not stand out as a suspicious event, but maybe Powershell logs can be the source of a flag if that is not their normal method to log on. 2.6.e Hashes = Using hashes from the submitted samples, Malwr.com will attempt to match the file with any previously known malware. If it finds a match, the results from that will be shown. Otherwise it will run the sample through its sandbox.

2.6.f URI / URL**A.**



```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"MALWARE-BACKDOOR phpMyAdmin server_sync.php backdoor access attempt"; flow:to_server,established; content:"/phpMyAdmin/server_sync.php"; fast_pattern:only; http_uri; metadata:impact_flag red, policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,55672; reference:cve,2012-5159; reference:url,osvdb.org/show/osvdb/85739; reference:url,phpmyadmin.net/home_page/security/PMASA-2012-5.php; classtype:trojan-activity; sid:24256; rev:5;)
/nsm/server_data/securityonion/rules/so-eth1-1/downloaded.rules: Line 20767
```

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
	209.165.200.235	172.16.1.10	4	5	0	233	45438	2	0	63	16869

TCP	Source Port	Dest Port	R 1	R 0	U R G	A C K	P S H	R S T	S Y N	F I N	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
	59478	80	.	.	.	X	X	.	.	.	983305273	3329932407	8	0	83	0	24112

DATA

```
47 45 54 20 2F 33 72 64 70 61 72 74 79 2F 70 68    GET /3rdparty/ph
70 4D 79 41 64 6D 69 6E 2F 73 65 72 76 65 72 5F    pMyAdmin/server_
73 79 6E 63 2E 70 68 70 3F 63 3D 70 68 70 69 6E    sync.php?c=phpin
66 6F 28 29 20 48 54 54 50 2F 31 2E 31 0D 0A 48    fo() HTTP/1.1..H
6F 73 74 3A 20 77 77 77 2E 61 62 63 2E 70 75 62    ost: www.abc.pub
6C 69 63 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A    lic..User-Agent:
20 4D 6F 7A 69 6C 6C 61 2F 35 2E 30 30 20 28 4E     Mozilla/5.00 (N
69 6B 74 6F 2F 32 2F 31 2F 36 29 20 28 45 76 61    ikto/2.1.6) (Eva
```

Q. 2.7 Map the provided events to these source technologies

A. It would be good to know the Type of Log vs. Device That Produced It

2.7.a NetFlow
2.7.b IDS / IPS
2.7.c Firewall
2.7.d Network application control
2.7.e Proxy logs
2.7.f Antivirus

Q. 2.8 Compare and contrast impact and no impact for these items
2.8.a False Positive
2.8.b False Negative
2.8.c True Positive
2.8.d True Negative

A. All decisions of security controls can be classified as one of the following:

- **False negative:** The security control did not detect actual malicious activity. Minimizing false negatives should be given a very high priority, sometimes at the expense of higher occurrences of false positives.

- **False positive:** The security control acted as a consequence of benign (non-malicious) activity. Many false positives can significantly drain the SOC resources.

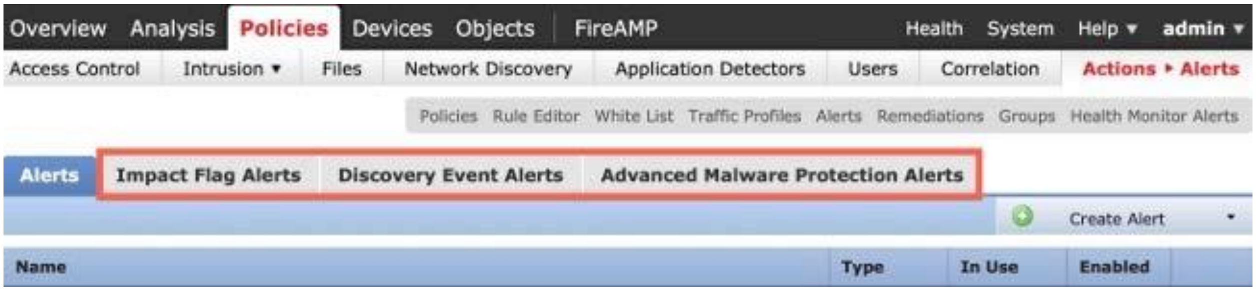
- **True negative:** The security control has not acted, because there was no malicious activity, which represents normal and optimal operation.

- **True positive:** The security control acted as a consequence of malicious activity, which represents normal and optimal operation.

An effective security control should produce true positive events, less false positive events, and most importantly, minimal amounts of false negative events.

Q. 2.9 Interpret a provided intrusion event and host profile to calculate the impact flag generated by Firepower Management Center (FMC)

A. You can also configure a FireSIGHT Management Center to send syslog alerts for events with a specific impact flag, specific type of discovery events and malware events. In order to do that, you have to create a syslog alert and then configure the type of events that you want to send to your syslog server. You can do that by navigating to the **Policies > Actions > Alerts** page, and then selecting a tab for the desired alert type.



If your FireSIGHT System deployment includes a FireSIGHT license, you can view *indications of compromise* (IOC) in the host profile. These indications correlate various types of data (intrusion events, Security Intelligence, connection events, and file or malware events) associated with hosts to determine whether a host on your monitored network is likely to be compromised by malicious means. From the host profile, you can see an overview of a host's IOC tags, view the events associated with IOC, mark IOC tags resolved, and edit IOC rule states in the discovery policy.

3.0 Incident Response

Q. 3.1 Describe the elements that should be included in an incident response plan as stated in NIST.SP800-61 r2

A. Policy Elements Policy governing incident response is highly individualized to the organization. However, most policies include the same key elements:

- Statement of management commitment
- Purpose and objectives of the policy
- Scope of the policy (to whom and what it applies and under what circumstances)
- Definition of computer security incidents and related terms

- Organizational structure and definition of roles, responsibilities, and levels of authority; should include the authority of the incident response team to confiscate or disconnect equipment and to monitor suspicious activity, the requirements for reporting certain types of incidents, the requirements and guidelines for external communications and information sharing (e.g., what can be shared with whom, when, and over what channels), and the handoff and escalation points in the incident management process
- Prioritization or severity ratings of incidents Performance measures (as discussed in Section 3.4.2) Reporting and contact forms.

3.2 Map elements to these steps of analysis based on the NIST.SP800-61 r2 **Q.**
3.2.a Preparation

A. Chapter 13 Section 3 = **Preparation**: The goal of the preparation phase is to get the company's team and resources ready to handle a security incident.

Preparation may include the following:

1. Educating the users and IT staff to respond to computer and network security incidents quickly and correctly.
2. Developing and maintaining all the proper documentation, such as network diagrams, configuration standards, change control documentations, and so on.
3. Planning for the logged and captured data retention period, who does what during an incident, and setting up the proper roles and responsibilities (RACI).

Q. 3.2.b Detection and analysis

A. Chapter 13 Section 3 = **Identification:** The SOC analyst performs continuous monitoring, and active cyber threat hunting. When a true positive incident has been detected, the incident response team is activated. During the investigation process, the SOC analyst or the incident response team may also contact the CERT/CC, or other security intelligence sources, which tracks Internet security activity and has the most current threat information.

Analysis: The incident response team should work quickly to analyze and validate each incident, following a pre-defined process and documenting each step that is taken. When the team believes that an incident has occurred, the team should rapidly perform an initial analysis to determine the incident's scope.

The initial analysis may include:

1. Which networks, systems, or applications are affected?
2. Who or what originated the incident?
3. What tools or attack methods are being used?
4. Which vulnerabilities are being exploited?

The initial analysis should provide enough information for the team to prioritize subsequent activities, such as containment of the incident and deeper analysis of the effects of the incident (if required, this deeper analysis may occur after the containment phase).

Q. 3.2.c Containment, eradication, and recovery
A. Chapter 13 Section 3 = **Containment:** Incident containment is perhaps the hardest and most important decision that is made during an incident.

Decision points for containment may include:

1. What is the scope of the incident?
2. What is the type of device?
3. What is the network reachability of the device that has been affected by the incident?
4. How quickly the incident response team can get containment in place?
5. How quickly containment is needed?

Last, but not least, is the reality that not all incidents are created equal and neither are containment options. The broader picture must be considered. For example, if data exfiltration is currently taking place, the incident response team may need to move quickly to contain and minimize the damage.

Without taking the time initially to understand each facet of containment, documenting them, testing them, and knowing the available fallback options, it is likely that the incident response team will fumble in making such a critical decision. Also, if the containment's impact on the business is not well understood, containment may do more harm than good.

Eradication and recovery: The incident response team investigates to find the origin of the incident. The root cause of the problem and all traces of potentially malicious code are removed, which may also involve changing passwords for accounts, hardening systems, and so on. Data and software are restored from clean backup files, ensuring that no vulnerabilities remain. After recovery, the systems are monitored for any sign of weakness and incident recurrence. Recovery may also involve tactical fixes including user account changes, patching software, and device hardening, and prioritizing strategic fixes such as process changes.

Q. 3.2.d Post-incident analysis (lessons learned)
A. Chapter 13 Section 3 = **Lessons learned:** The incident response team analyzes how and why the incident happened and performs an FMEA against it. FMEA is a qualitative and systematic tool, usually created within a spreadsheet, to help practitioners anticipate what might go wrong with a product or process. This phase includes documenting how the incident was handled, recommendations for better future response, and how to prevent a recurrence.

Q. 3.3 Map the organization stakeholders against the NIST IR categories (C2M2, NIST.SP800-61 r2)
3.3.a Preparation, .b Detection and analysis, .c Containment, eradication, and recovery
.d Post-incident analysis (lessons learned)

A. The C2M2 enables organizations to evaluate cybersecurity capabilities consistently, communicate capability levels in meaningful terms, and prioritize cybersecurity investments. The model can be used by any organization, regardless of ownership, structure, size, or industry. Within the organization, various stakeholders may benefit from familiarity with the model. This document specifically targets people in the following organizational roles:

- Decision makers (executives) who control the allocation of resources and the management of risk in organizations; these are typically senior leaders
- Leaders with responsibility for managing organizational resources and operations associated with the domains of this model (see Section 3.1 for more information on the content of each C2M2 domain)
- Practitioners with responsibility for supporting the organization in the use of this model (planning and managing changes in the organization based on the model)
- Facilitators with responsibility for leading a self-evaluation of the organization based on this model and the associated toolkit and analyzing the self-evaluation results.
  Generally speaking, a facilitator is someone who helps a group of people understand their common objectives and assists them in planning to achieve these objectives without taking a particular position in the discussion.

3.4 Describe the goals of the given CSIRT
3.4.a Internal CSIRT
3.4.b National CSIRT
3.4.c Coordination centers
3.4.d Analysis centers

3.4.e Vendor teams
3.4.f Incident response providers (MSSP)

A. Chapter 14 Section 2 = CSIRTs come in all shapes and sizes and serve diverse constituencies. Some general categories of CSIRTs include, but are not limited to, the following:

- **Internal CSIRTs** provide incident handling services to their parent organization, which could be a CSIRT for a bank, a manufacturing company, a university, or a federal agency.

- **National CSIRTs** provide incident handling services to a country. Examples include JPCERT/CC orSingCERT. A list of national CSIRTs can be found at: http://www.cert.org/incident-management/national-csirts/national-csirts.cfm.

- **Coordination centers** coordinate and facilitate the handling of incidents across various CSIRTs. Examples include the CERT Coordination Center or US-CERT.

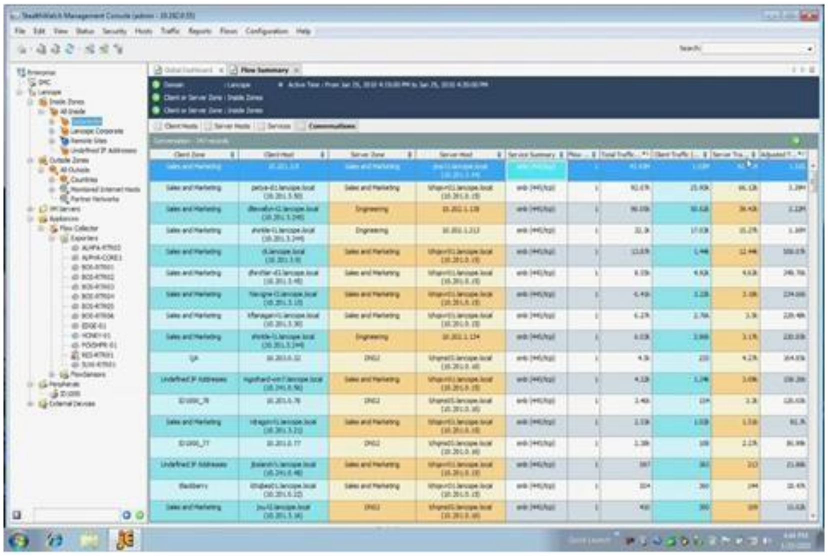
- **Analysis centers** focus on synthesizing data from various sources to determine trends and patterns in incident activity. This information can be used to help predict future activity or to provide early warning when the activity matches a set of previously determined characteristics.

- **Vendor teams** handle reports of vulnerabilities in their software or hardware products. They may work within the organization to determine if their products are vulnerable and to develop remediation and mitigation strategies. A vendor team may also be the internal CSIRT for a vendor organization. For example, the Cisco Product Security Incident Response Team (Cisco PSIRT) is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information related to Cisco products and networks. Cisco PSIRT provides security advisories and security responses.**Incident response providers** offer incident handling services as a for-fee service to other organizations.

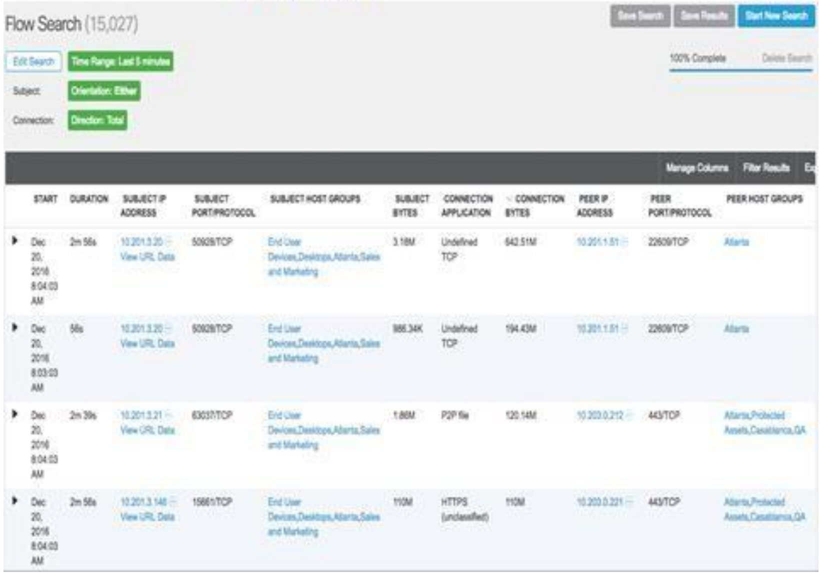
Q. Identify these elements used for network profiling
3.5.a Total throughput
3.5.b Session duration
3.5.c Ports used
3.5.d Critical asset address space

A. Chapter 1

NETFLOW COLLECTOR OUTPUT



NETFLOW



Flow Search (15,027)

Time Range: Last 5 minutes

Subject: Orientation: Either

Connection: Direction: Total

	START	DURATION	SUBJECT IP ADDRESS	SUBJECT PORT/PROTOCOL	SUBJECT HOST GROUPS	SUBJECT BYTES	CONNECTION APPLICATION	CONNECTION BYTES	PEER IP ADDRESS	PEER PORT/PROTOCOL	PEER HOST GROUPS
▶	Dec 20, 2016 8:04:03 AM	2m 56s	10.201.3.20 View URL Data	50928/TCP	End User Devices,Desktops,Atlanta,Sales and Marketing	3.18M	Undefined TCP	642.51M	10.201.1.51	22609/TCP	Atlanta
▶	Dec 20, 2016 8:03:03 AM	56s	10.201.3.20 View URL Data	50928/TCP	End User Devices,Desktops,Atlanta,Sales and Marketing	986.34K	Undefined TCP	194.43M	10.201.1.51	22609/TCP	Atlanta
▶	Dec 20, 2016 8:04:03 AM	2m 39s	10.201.3.21 View URL Data	63037/TCP	End User Devices,Desktops,Atlanta,Sales and Marketing	1.86M	P2P file	120.14M	10.203.0.212	443/TCP	Atlanta,Protected Assets,Casablanca,QA
▶	Dec 20, 2016 8:04:03 AM	2m 56s	10.201.3.146 View URL Data	15661/TCP	End User Devices,Desktops,Atlanta,Sales and Marketing	110M	HTTPS (unclassified)	110M	10.203.0.221	443/TCP	Atlanta,Protected Assets,Casablanca,QA

Q. 3.6 Identify these elements used for server profiling

3.6.a Listening ports

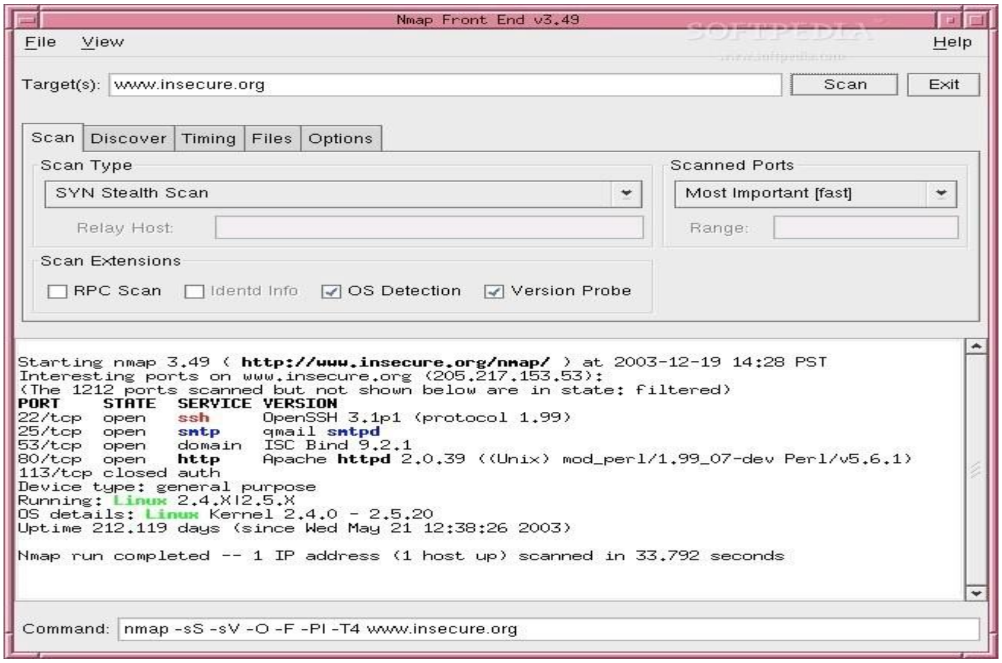
3.6.b Logged in users/service accounts

3.6.c Running processes

3.6.d Running tasks

3.6.e Applications

A. Chapter 1 Slides 9, 10



Target(s): www.insecure.org

Scan Type: SYN Stealth Scan

Scanned Ports: Most Important [fast]

□ RPC Scan □ Identd Info ☑ OS Detection ☑ Version Probe

```
Starting nmap 3.49 ( http://www.insecure.org/nmap/ ) at 2003-12-19 14:28 PST
Interesting ports on www.insecure.org (205.217.153.53):
(The 1212 ports scanned but not shown below are in state: filtered)
PORT     STATE  SERVICE VERSION
22/tcp   open   ssh     OpenSSH 3.1p1 (protocol 1.99)
25/tcp   open   smtp    qmail smtpd
53/tcp   open   domain  ISC Bind 9.2.1
80/tcp   open   http    Apache httpd 2.0.39 ((Unix) mod_perl/1.99_07-dev Perl/v5.6.1)
113/tcp  closed auth
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux Kernel 2.4.0 - 2.5.20
Uptime 212.119 days (since Wed May 21 12:38:26 2003)

Nmap run completed -- 1 IP address (1 host up) scanned in 33.792 seconds
```

Command: nmap -sS -sV -O -F -PI -T4 www.insecure.org

3.7 Map data types to these compliance frameworks

Q. 3.7.a PCI **A.** see data types in question 3.8 below

Q. 3.7.b HIPPA (Health Insurance Portability and Accountability Act)

A. Protected Health Information
"Health information means any information, whether oral or recorded in any form or medium, that– (A) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
(B) relates to the past, present, or future physical or mental health or condition of any individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual."
(i) That identifies the individual; or With respect to which there is a reasonable basis to believe the information can be used to identify the individual."
(i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium.
(2) *Protected health information* excludes individually identifiable health information in:(i) Education

records (ii) Employment records held by a covered entity in its role as employer."

Q. 3.7.c SOX

A. Any financial information needs to be safeguarded, and its integrity assured. Specific internal security controls need to be identified that protect this data, auditing must take place, and this security posture reassessed every year – including any changes or deficiencies as a result of changing conditions. Organizations must enable safeguards to audit the integrity of financial data across widespread heterogeneous infrastructures. The combination of encryption, integrated key management and access controls meets the needs for creating and maintaining access controls to financial data.

Q. 3.8 Identify data elements that must be protected with regards to a specific standard (PCI- DSS)

A. Cardholder data refers to any information contained on a customer's payment card. The data is printed on either side of the card and is contained in digital format on the magnetic stripe embedded in the backside of the card. Some payment cards store data in chips embedded on the front side. The front side usually has the primary account number (PAN), cardholder name and expiration date. The magnetic stripe or chip holds these plus other sensitive data for authentication and authorization. In general, no payment card data should ever be stored by a merchant unless it's necessary to meet the needs of the business. Sensitive data on the magnetic stripe or chip must never be stored. Only the PAN, expiration date, service code, or cardholder name may be stored, and merchants must use technical precautions for safe storage.

4.0 Data and Event Analysis

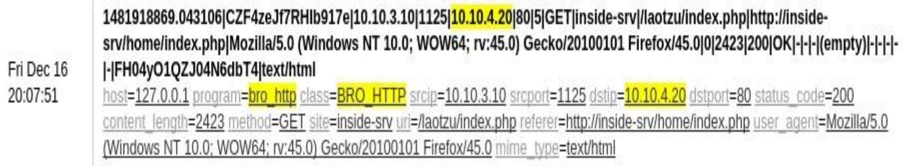
4.1 Describe the process of data normalization

Normalization is the process of manipulating security event data and fitting it into a common schema. Security event monitoring systems must provide parsers that are designed to work with each of the different data sources. The parsers algorithmically take the event data and extract the relevant characteristics and fill in the appropriate fields in the common schema

4.2 Interpret common data values into a universal format

Security Data Normalization Cont.

- ELSA has parsed an HTTP transaction event that is produced by Bro
- - format of this log entry is completely different than the firewall log message
- - relevant data is parsed out of the log entry and placed in the common schema
- - IP 5-tuple information has been parsed into the same fields that were used for the firewall syslog message.
- Other fields that are associated with HTTP transactions are the following:
- Method
- Site
- URL (IT IS SOMETIMES DIFFICULT TO IDENTIFY URL VS. REFERER)
- Referer
- User_agent

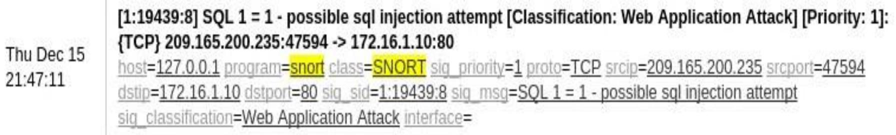


```
Fri Dec 16   1481918869.043106|CZF4zeJf7RHIb917e|10.10.3.10|1125|10.10.4.20|80|5|GET|inside-srv|/laotzu/index.php|http://inside-
20:07:51     srv/home/index.php|Mozilla/5.0 (Windows NT 10.0; WOW64; rv:45.0) Gecko/20100101 Firefox/45.0|0|2423|200|OK|-|-|-|(empty)|-|-|-|-
             |-|FH04yO1QZJ04N6dbT4|text/html
             host=127.0.0.1 program=bro_http class=BRO_HTTP srcip=10.10.3.10 srcport=1125 dstip=10.10.4.20 dstport=80 status_code=200
             content_length=2423 method=GET site=inside-srv uri=/laotzu/index.php referer=http://inside-srv/home/index.php user_agent=Mozilla/5.0
             (Windows NT 10.0; WOW64; rv:45.0) Gecko/20100101 Firefox/45.0 mime_type=text/html
```

4.3 Describe 5-tuple correlation

Security Data Normalization Cont.

- As a third example, consider the Snort alert that is shown below
- - completely different format
- - data has been extracted and placed into the common schema •
  - IP 5-tuple uses the proto, srcip, srcport, dstip, and dstport fields.
- - fields that are uniquely associated with IPS alert messages:
- sig_sid
- sig_msg
- sig_classification



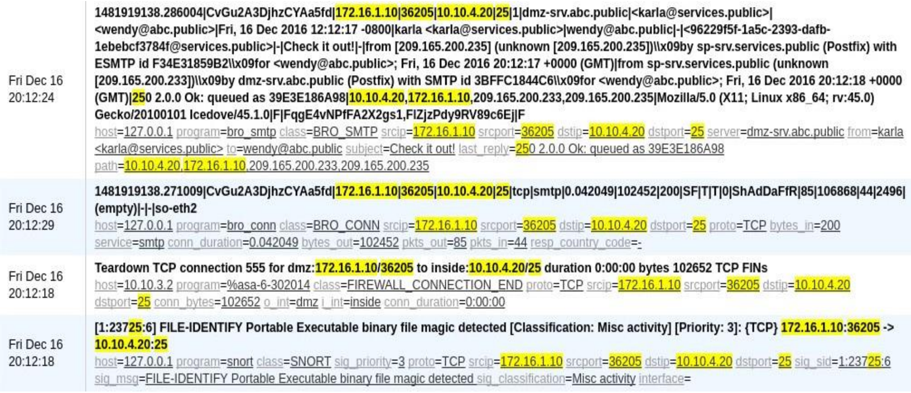
```
Thu Dec 15   [1:19439:8] SQL 1 = 1 - possible sql injection attempt [Classification: Web Application Attack] [Priority: 1]:
21:47:11     {TCP} 209.165.200.235:47594 -> 172.16.1.10:80
             host=127.0.0.1 program=snort class=SNORT sig_priority=1 proto=TCP srcip=209.165.200.235 srcport=47594
             dstip=172.16.1.10 dstport=80 sig_sid=1:19439:8 sig_msg=SQL 1 = 1 - possible sql injection attempt
             sig_classification=Web Application Attack interface=
```

4.4 Describe the 5-tuple approach to isolate a compromised host in a grouped set of logs

Event Correlation

- Correlation
- - relationship or connection between two or more things

- - recognizing that two or more security events are related • - leveraging the relationship to further the process of analysis.
- - IP 5-tuple to correlate events
- - IPS alert provides an initial IP 5-tuple of interest
- - data is already normalized
- - query the database with the IP 5-tuple to produce a report of correlated data • - the figure is the result of this ELSA query:



```
Fri Dec 16   1481919138.286004|CvGu2A3DjhzCYAa5fd|172.16.1.10|36205|10.10.4.20|25|1|dmz-srv.abc.public|<karla@services.public>|
20:12:24     <wendy@abc.public>|Fri, 16 Dec 2016 12:12:17 -0800|karla <karla@services.public>|wendy@abc.public|-|<96229f5f-1a5c-2393-dafb-
             1ebebcf3784f@services.public>|-|Check it out!|-|from [209.165.200.235] (unknown [209.165.200.235])\\x09by sp-srv.services.public (Postfix) with
             ESMTP id F34E31859B2\\x09for <wendy@abc.public>; Fri, 16 Dec 2016 20:12:17 +0000 (GMT)|from sp-srv.services.public (unknown
             [209.165.200.233])\\x09by dmz-srv.abc.public (Postfix) with SMTP id 3BFFC1844C6\\x09for <wendy@abc.public>; Fri, 16 Dec 2016 20:12:18 +0000
             (GMT)|250 2.0.0 Ok: queued as 39E3E186A98|10.10.4.20,172.16.1.10,209.165.200.233,209.165.200.235|Mozilla/5.0 (X11; Linux x86_64; rv:45.0)
             Gecko/20100101 Icedove/45.1.0|F|FqgE4vNPfFA2X2gs1,FIZjzPdy9RV89c6Ej|F
             host=127.0.0.1 program=bro_smtp class=BRO_SMTP srcip=172.16.1.10 srcport=36205 dstip=10.10.4.20 dstport=25 server=dmz-srv.abc.public from=karla
             <karla@services.public> to=wendy@abc.public subject=Check it out! last_reply=250 2.0.0 Ok: queued as 39E3E186A98
             path=10.10.4.20,172.16.1.10,209.165.200.233,209.165.200.235

Fri Dec 16   1481919138.271009|CvGu2A3DjhzCYAa5fd|172.16.1.10|36205|10.10.4.20|25|tcp|smtp|0.042049|102452|200|SF|T|T|0|ShAdDaFfR|85|106868|44|2496|
20:12:29     (empty)|-|-|so-eth2
             host=127.0.0.1 program=bro_conn class=BRO_CONN srcip=172.16.1.10 srcport=36205 dstip=10.10.4.20 dstport=25 proto=TCP bytes_in=200
             service=smtp conn_duration=0.042049 bytes_out=102452 pkts_out=85 pkts_in=44 resp_country_code=-

Fri Dec 16   Teardown TCP connection 555 for dmz:172.16.1.10/36205 to inside:10.10.4.20/25 duration 0:00:00 bytes 102652 TCP FINs
20:12:18     host=10.10.3.2 program=%asa-6-302014 class=FIREWALL_CONNECTION_END proto=TCP srcip=172.16.1.10 srcport=36205 dstip=10.10.4.20
             dstport=25 conn_bytes=102652 o_int=dmz i_int=inside conn_duration=0:00:00

Fri Dec 16   [1:23725:6] FILE-IDENTIFY Portable Executable binary file magic detected [Classification: Misc activity] [Priority: 3]: {TCP} 172.16.1.10:36205 ->
20:12:18     10.10.4.20:25
             host=127.0.0.1 program=snort class=SNORT sig_priority=3 proto=TCP srcip=172.16.1.10 srcport=36205 dstip=10.10.4.20 dstport=25 sig_sid=1:23725:6
             sig_msg=FILE-IDENTIFY Portable Executable binary file magic detected sig_classification=Misc activity interface=
```

Event Correlation Cont.

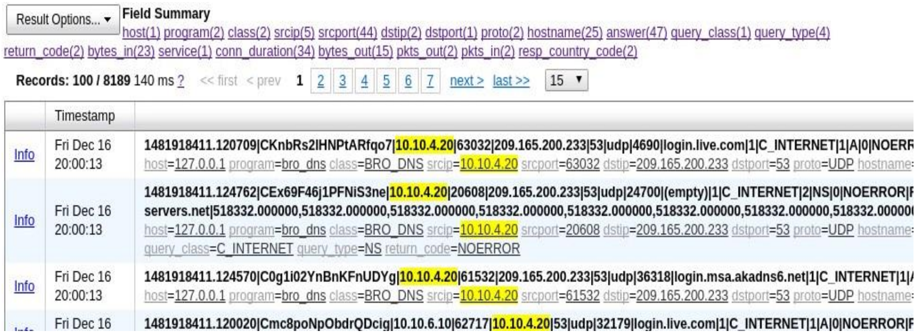
- An SMTP transaction record that is produced by Bro.
- A TCP connection record that is produced by Bro.
- A TCP connection record that is produced by a Cisco Adaptive Security Appliance (Cisco ASA) firewall.
- An alert that is produced by Snort.
- Related to the previous graphic there are four matching events in the ELSA database. From top to bottom the events are as follows:

- Being associated with the same IP 5-tuple indicates a very strong relationship between these events
- - important thing to recognize is that correlated events provide much more detail and context to the analyst than can be obtained from any single event.
- - leverage weaker correlations
- - IPS alert
- - internal system connects to an exploit kit landing page
- - determine whether the exploit kit actually delivered an exploit
- - HTTP transaction log which documents the exploit kit interaction
- - HTTP redirect from the exploit kit landing page to a malware download on a completely different web site
- - HTTP transactions between the client and the target of the redirection is now of interest
- - there is a correlation between these sets of events.

Other Security Data Manipulation

Aggregation

- a data mining technique where data is gathered to get information about particular variables
- - all records that share a single, common variable
- - ELSA may be queried with simply an IP address
- - over 8,000 matching records
- - finding those few new records of interest among over 8,000 records in the list is going to be a challenge. The figure below is the result of this ELSA query:

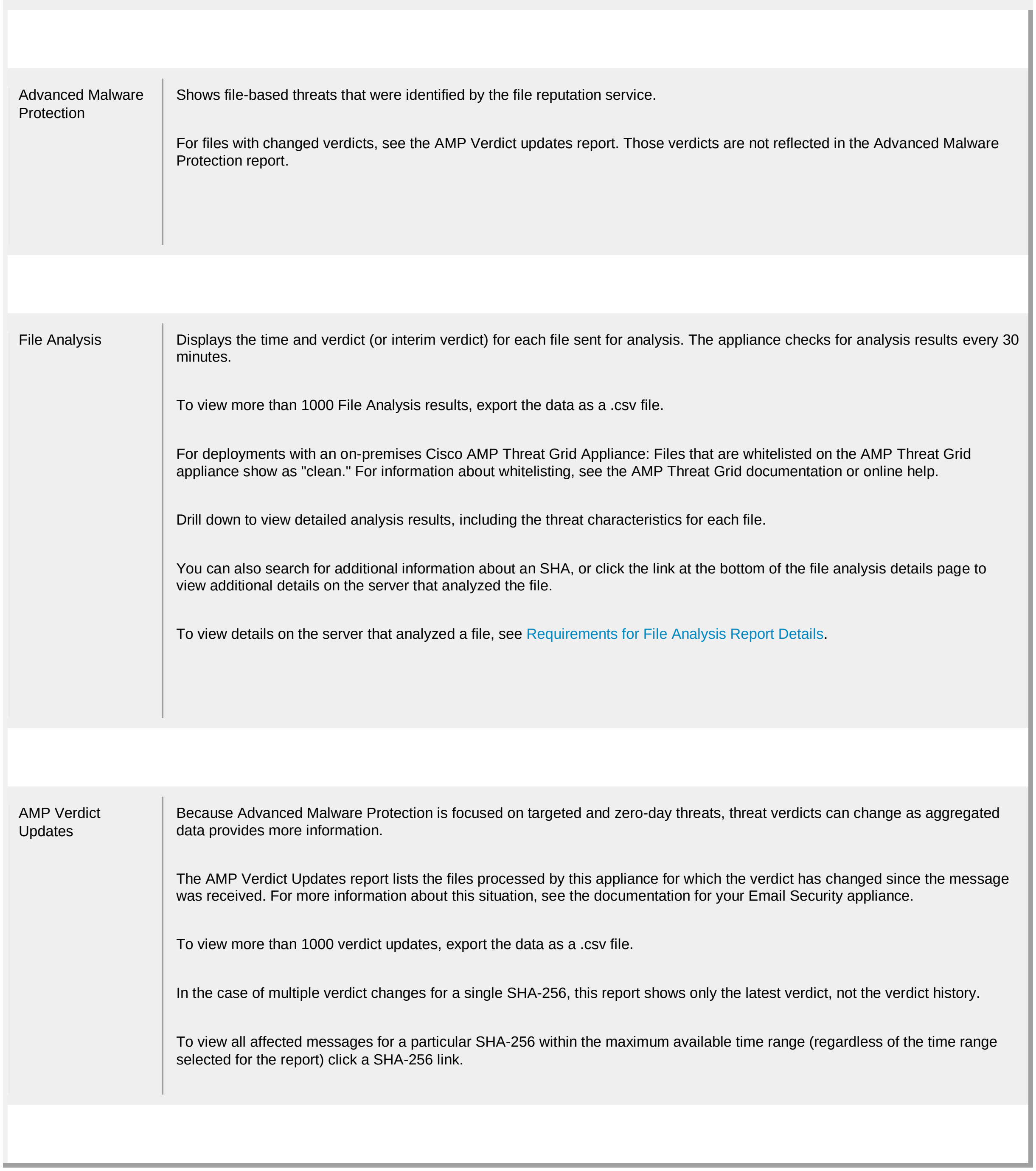


```
Field Summary
host(1) program(2) class(2) srcip(5) srcport(44) dstip(2) dstport(1) proto(2) hostname(25) answer(47) query_class(1) query_type(4)
return_code(2) bytes_in(23) service(1) conn_duration(34) bytes_out(15) pkts_out(2) pkts_in(2) resp_country_code(2)

Records: 100 / 8189 140 ms ?   << first  < prev   1  2  3  4  5  6  7  next >  last >>   15 ▾

      Timestamp
Info  Fri Dec 16  1481918411.120709|CKnbRs2IHNPtARfqo7|10.10.4.20|63032|209.165.200.233|53|udp|4690|login.live.com|1|C_INTERNET|1|A|0|NOERR
      20:00:13    host=127.0.0.1 program=bro_dns class=BRO_DNS srcip=10.10.4.20 srcport=63032 dstip=209.165.200.233 dstport=53 proto=UDP hostname=
                  1481918411.124762|CEx69F46j1PFNiS3ne|10.10.4.20|20608|209.165.200.233|53|udp|24700|(empty)|1|C_INTERNET|2|NS|0|NOERROR|F
Info  Fri Dec 16  servers.net|518332.000000,518332.000000,518332.000000,518332.000000,518332.000000,518332.000000,518332.000000,518332.00000
      20:00:13    host=127.0.0.1 program=bro_dns class=BRO_DNS srcip=10.10.4.20 srcport=20608 dstip=209.165.200.233 dstport=53 proto=UDP hostname=
                  query_class=C_INTERNET query_type=NS return_code=NOERROR
Info  Fri Dec 16  1481918411.124570|C0g1i02YnBnKFnUDYg|10.10.4.20|61532|209.165.200.233|53|udp|36318|login.msa.akadns6.net|1|C_INTERNET|1|
      20:00:13    host=127.0.0.1 program=bro_dns class=BRO_DNS srcip=10.10.4.20 srcport=61532 dstip=209.165.200.233 dstport=53 proto=UDP hostname=
      Fri Dec 16  1481918411.120020|Cmc8poNpObdrQDcig|10.10.6.10|62717|10.10.4.20|53|udp|32179|login.live.com|1|C_INTERNET|1|A|0|NOERROR|F
```

4.5 Describe the retrospective analysis method to find a malicious file, provided file analysis report

A retrospective analysis or retrospective study is a research method that is used when the outcome of an event is already known.

Report	Description

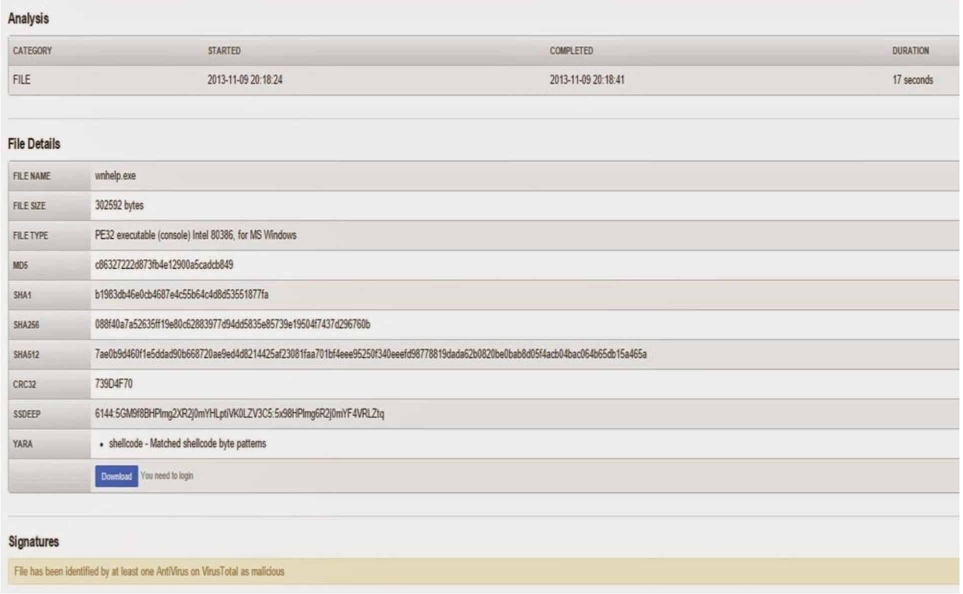


Advanced Malware Protection	Shows file-based threats that were identified by the file reputation service. For files with changed verdicts, see the AMP Verdict updates report. Those verdicts are not reflected in the Advanced Malware Protection report.
File Analysis	Displays the time and verdict (or interim verdict) for each file sent for analysis. The appliance checks for analysis results every 30 minutes. To view more than 1000 File Analysis results, export the data as a .csv file. For deployments with an on-premises Cisco AMP Threat Grid Appliance: Files that are whitelisted on the AMP Threat Grid appliance show as "clean." For information about whitelisting, see the AMP Threat Grid documentation or online help. Drill down to view detailed analysis results, including the threat characteristics for each file. You can also search for additional information about an SHA, or click the link at the bottom of the file analysis details page to view additional details on the server that analyzed the file. To view details on the server that analyzed a file, see Requirements for File Analysis Report Details.
AMP Verdict Updates	Because Advanced Malware Protection is focused on targeted and zero-day threats, threat verdicts can change as aggregated data provides more information. The AMP Verdict Updates report lists the files processed by this appliance for which the verdict has changed since the message was received. For more information about this situation, see the documentation for your Email Security appliance. To view more than 1000 verdict updates, export the data as a .csv file. In the case of multiple verdict changes for a single SHA-256, this report shows only the latest verdict, not the verdict history. To view all affected messages for a particular SHA-256 within the maximum available time range (regardless of the time range selected for the report) click a SHA-256 link.

4.6 Identify potentially compromised hosts within the network based on a threat analysis report containing malicious IP address or domains

SANDBOX CONT'D

A MALICIOUS FILE - SHELLCODE



Analysis

CATEGORY	STARTED	COMPLETED	DURATION
FILE	2013-11-09 20:18:24	2013-11-09 20:18:41	17 seconds

File Details

FILE NAME	wnhelp.exe
FILE SIZE	302592 bytes
FILE TYPE	PE32 executable (console) Intel 80386, for MS Windows
MD5	c86327222d873fb4e12900a5cadcb849
SHA1	b1983db46e0cb4687e4c55b64c4d8d53551877fa
SHA256	088f40a7a52635ff19e80c62883977d94dd5835e85739e19504f7437d296760b
SHA512	7ae0b9d460f1e5ddad90b668720ae9ed4d8214425af23081faa701bf4eee95250f340eeefd98778819dada62b0820be0bab8d05f4acb04bac064b65db15a465a
CRC32	739D4F70
SSDEEP	6144:5GM9f8BHPlmg2XR2j0mYHLptiVK0LZV3C5:5x98HPlmg6R2j0mYF4VRLZtq
YARA	• shellcode - Matched shellcode byte patterns
	Download You need to login

Signatures

File has been identified by at least one AntiVirus on VirusTotal as malicious

MALICIOUS FILES

Where did the malware come from?

What was the method and point of entry?

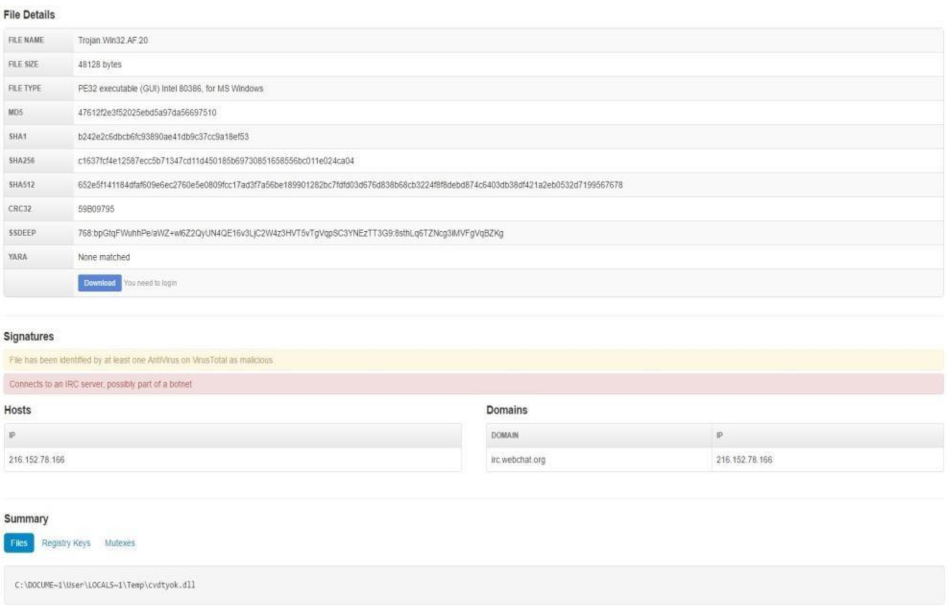
Where has it been and what systems were affected?

What did the threat do and what is it doing now?

How is the threat stopped and root cause eliminated?

MALICIOUS FILES CONT’D.

This report points to a file named cvdtyok.dll. It is identified as a Trojan



File Details

FILE NAME	Trojan.Win32.AF.20
FILE SIZE	48128 bytes
FILE TYPE	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	47612f2e3f52025ebd5a97da56697510
SHA1	b242e2c6dbcb6fc93890ae41db9c37cc9a18ef53
SHA256	c1637fcf4e12587ecc5b71347cd11d450185b69730851658556bc011e024ca04
SHA512	652e5f141184dfaf609e6ec2760e5e0809fcc17ad3f7a56be189901282bc7fdfd03d676d838b68cb3224f8f8debd874c6403db38df421a2eb0532d7199567678
CRC32	59B09795
SSDEEP	768:bpGtqFWuhhPe/aWZ+wl6Z2QyUN4QE16v3LjC2W4z3HVT5vTgVqpSC3YNEzTT3G9:8sthLq6TZNcg3iMVFgVqBZKg
YARA	None matched
	Download You need to login

Signatures

File has been identified by at least one AntiVirus on VirusTotal as malicious

Connects to an IRC server, possibly part of a botnet

Hosts

IP
216.152.78.166

Domains

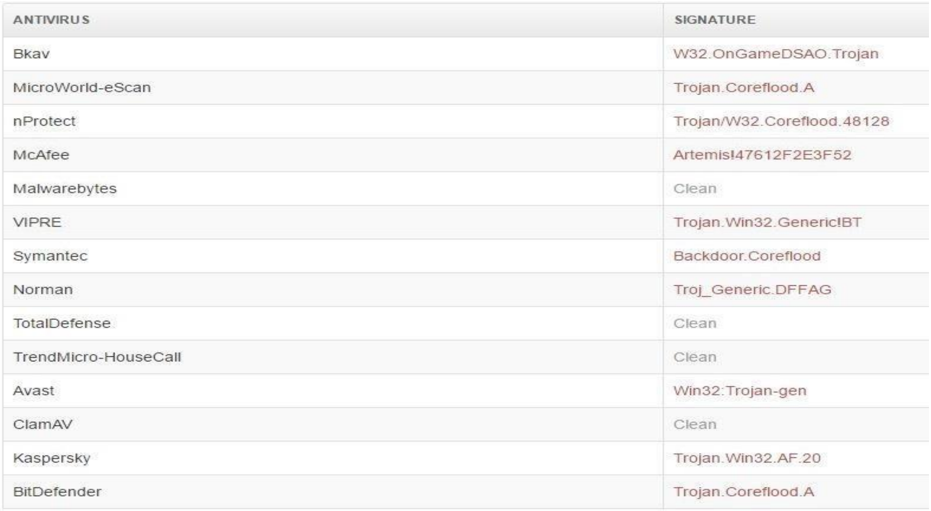
DOMAIN	IP
irc.webchat.org	216.152.78.166

Summary

```
C:\DOCUME~1\User\LOCALS~1\Temp\cvdtyok.dll
```

MALICIOUS FILES CONT'D.

THIS IS THE WAY SOME TOOLS SEE THE FILE



ANTIVIRUS	SIGNATURE
Bkav	W32.OnGameDSAO.Trojan
MicroWorld-eScan	Trojan.Coreflood.A
nProtect	Trojan/W32.Coreflood.48128
McAfee	Artemis!47612F2E3F52
Malwarebytes	Clean
VIPRE	Trojan.Win32.Generic!BT
Symantec	Backdoor.Coreflood
Norman	Troj_Generic.DFFAG
TotalDefense	Clean
TrendMicro-HouseCall	Clean
Avast	Win32:Trojan-gen
ClamAV	Clean
Kaspersky	Trojan.Win32.AF.20
BitDefender	Trojan.Coreflood.A

Coreflood to function as a back-door, keylogger, and botnet.

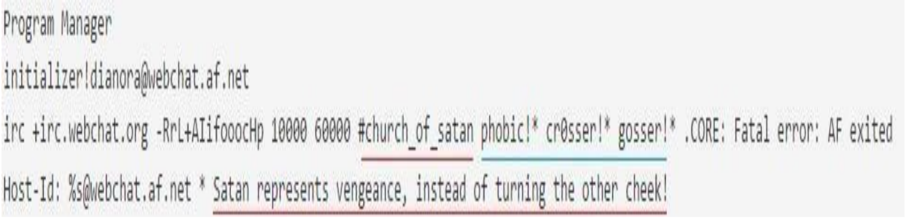
MALICIOUS FILES CONT'D

SAME FILE

Underlines in red are some lines that might not normally be included in legitimate software.

The name of an IRC channel and the channel's topic or message of the day can be surmised.

In blue, the handles or user names of some of the channel users who are involved in the creation of this malware can be seen.



```
Program Manager
initializer!dianora@webchat.af.net
irc +irc.webchat.org -RrL+AIifooocHp 10000 60000 #church_of_satan phobic!* cr0sser!* gosser!* .CORE: Fatal error: AF exited
Host-Id: %s@webchat.af.net * Satan represents vengeance, instead of turning the other cheek!
```

Q. 4.7 Map DNS logs and HTTP logs together to find a threat actor

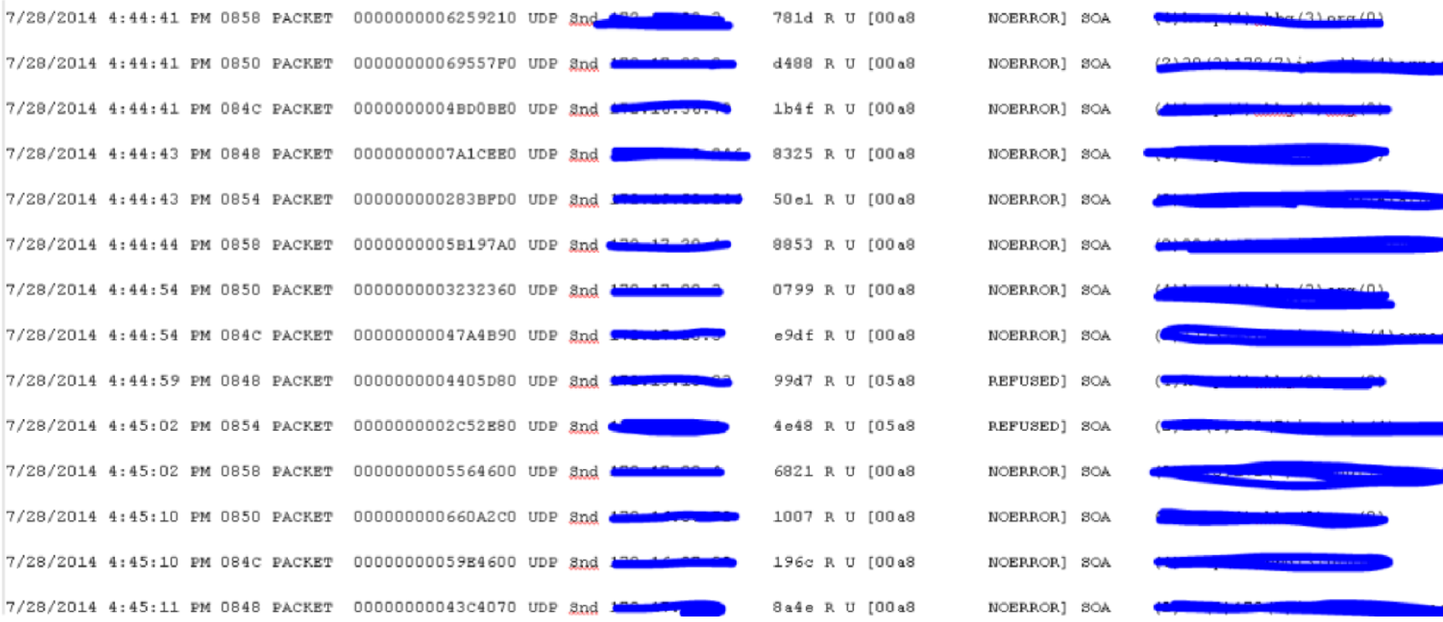
A. Think this means to be able to look at logs like the ones below and track IP addresses and Web site URLs that can be compared against a known list/profile of bad/malicious sites. Verify that your network may be communicating with malicious sites like in some command and control process.

Below is an example of an HTTP log file:

```
fcrawler.looksmart.com - - [26/Apr/2000:00:00:12 -0400] "GET /contacts.html HTTP/1.0" 200 4595 "-" "FASTWebCrawler/2.1-pre2 (ashen@looksmart.net)"
fcrawler.looksmart.com - - [26/Apr/2000:00:17:19 -0400] "GET /news/news.html HTTP/1.0" 200 16716 "-" "FASTWebCrawler/2.1-pre2 (ashen@looksmart.net)"

ppp931.on.bellglobal.com - - [26/Apr/2000:00:16:12 -0400] "GET /download/windows/asctab31.zip HTTP/1.0" 200 1540096 "http://www.htmlgoodies.com/downloads/freeware/webdevelopment/15.html" "Mozilla/4.7 [en]CSYMPA  (Win95; U)"

123.123.123.123 - - [26/Apr/2000:00:23:48 -0400] "GET /pics/wpaper.gif HTTP/1.0" 200 6248 "http://www.jafsoft.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"

123.123.123.123 - - [26/Apr/2000:00:23:47 -0400] "GET /asctortf/ HTTP/1.0" 200 8130 "http://search.netscape.com/Computers/Data_Formats/Document/Text/RTF" "Mozilla/4.05 (Macintosh; I; PPC)"

123.123.123.123 - - [26/Apr/2000:00:23:48 -0400] "GET /pics/5star2000.gif HTTP/1.0" 200 4005 "http://www.jafsoft.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"

123.123.123.123 - - [26/Apr/2000:00:23:50 -0400] "GET /pics/5star.gif HTTP/1.0" 200 1031 "http://www.jafsoft.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"

123.123.123.123 - - [26/Apr/2000:00:23:51 -0400] "GET /pics/a2hlogo.jpg HTTP/1.0" 200 4282 "http://www.jafsoft.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"
123.123.123.123 - - [26/Apr/2000:00:23:51 -0400] "GET /cgi-bin/newcount?jafsof3&width=4&font=digital&noshow HTTP/1.0" 200 36 "http://www.jafsoft.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"
```

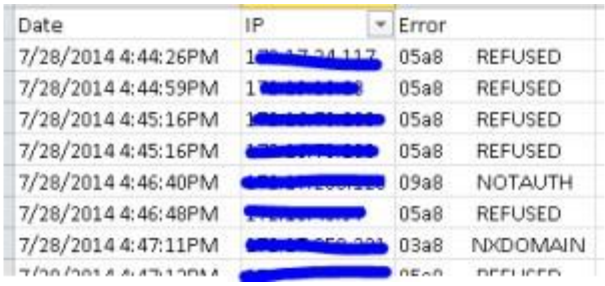
The first row of marked out lines is the IP address and the last row is the DNS record it attempted to updated. These were marked out for obvious reasons. Depending on the options you choose this log file can become enormous and isn't in the easiest format to read. What if I want to filter out just a single IP or narrow it down by a certain timeframe? You can't do that with the default log file. This is why I created a Powershell summary script.

Below is an example of a DNS log file:



```
7/28/2014 4:44:41 PM 0858 PACKET  0000000006259210 UDP Snd [redacted]  781d R U [00a8      NOERROR] SOA  [redacted]
7/28/2014 4:44:41 PM 0850 PACKET  00000000069557F0 UDP Snd [redacted]  d488 R U [00a8      NOERROR] SOA  [redacted]
7/28/2014 4:44:41 PM 084C PACKET  0000000004BD0BE0 UDP Snd [redacted]  1b4f R U [00a8      NOERROR] SOA  [redacted]
7/28/2014 4:44:43 PM 0848 PACKET  0000000007A1CEE0 UDP Snd [redacted]  8325 R U [00a8      NOERROR] SOA  [redacted]
7/28/2014 4:44:43 PM 0854 PACKET  000000000283BFD0 UDP Snd [redacted]  50e1 R U [00a8      NOERROR] SOA  [redacted]
7/28/2014 4:44:44 PM 0858 PACKET  0000000005B197A0 UDP Snd [redacted]  8853 R U [00a8      NOERROR] SOA  [redacted]
7/28/2014 4:44:54 PM 0850 PACKET  0000000003232360 UDP Snd [redacted]  0799 R U [00a8      NOERROR] SOA  [redacted]
7/28/2014 4:44:54 PM 084C PACKET  00000000047A4B90 UDP Snd [redacted]  e9df R U [00a8      NOERROR] SOA  [redacted]
7/28/2014 4:44:59 PM 0848 PACKET  0000000004405D80 UDP Snd [redacted]  99d7 R U [05a8      REFUSED] SOA  [redacted]
7/28/2014 4:45:02 PM 0854 PACKET  0000000002C52E80 UDP Snd [redacted]  4e48 R U [05a8      REFUSED] SOA  [redacted]
7/28/2014 4:45:02 PM 0858 PACKET  0000000005564600 UDP Snd [redacted]  6821 R U [00a8      NOERROR] SOA  [redacted]
7/28/2014 4:45:10 PM 0850 PACKET  00000000660A2C0 UDP Snd [redacted]  1007 R U [00a8      NOERROR] SOA  [redacted]
7/28/2014 4:45:10 PM 084C PACKET  00000000059E4600 UDP Snd [redacted]  196c R U [00a8      NOERROR] SOA  [redacted]
7/28/2014 4:45:11 PM 0848 PACKET  00000000043C4070 UDP Snd [redacted]  8a4e R U [00a8      NOERROR] SOA  [redacted]
```

The script below takes this log file and parses it out into a nice CSV file that looks like this:

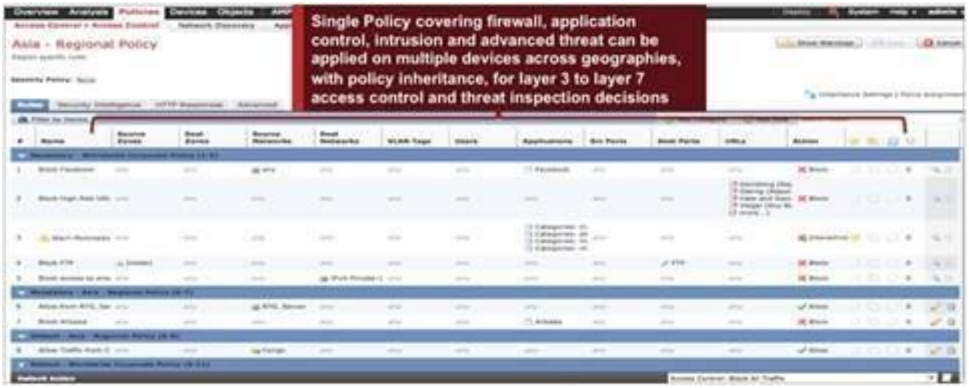


Date	IP	Error	
7/28/2014 4:44:26PM	[redacted]	05a8	REFUSED
7/28/2014 4:44:59PM	[redacted]	05a8	REFUSED
7/28/2014 4:45:16PM	[redacted]	05a8	REFUSED
7/28/2014 4:45:16PM	[redacted]	05a8	REFUSED
7/28/2014 4:46:40PM	[redacted]	09a8	NOTAUTH
7/28/2014 4:46:48PM	[redacted]	05a8	REFUSED
7/28/2014 4:47:11PM	[redacted]	03a8	NXDOMAIN
7/28/2014 4:47:12PM	[redacted]	05a8	REFUSED

Q. 4.8 Map DNS, HTTP, and threat intelligence data together

A. See answers on question 4.7 above. Map this log data to output from other sources to identify anomalies and threat actors.

Q. 4.9 Identify a correlation rule to distinguish the most significant alert from a given set of events from multiple data sources using the firepower management console



Single Policy covering firewall, application control, intrusion and advanced threat can be applied on multiple devices across geographies, with policy inheritance, for layer 3 to layer 7 access control and threat inspection decisions

Q. 4.10 Compare and contrast deterministic and probabilistic analysis

- **Deterministic Assessment Method:** The analyst should base their scenario assessment on a small or very limited set of assigned values and variables. This method relies on known data values to yield a single outcome for each proposed scenario. Due to the absolute nature of performing a deterministic assessment, minimum speculation is required in order to formulate an outcome.
- **Probabilistic Assessment Method:** The analyst should consider a wide range of probable scenarios which provide a distribution of all possible outcomes that can assist the analyst in determining the likelihood that an exploit will impact the network. Because the probabilistic model takes into account a wider range of probable scenarios and a higher degree of speculation, the probabilistic model is generally less accurate than the deterministic model.
- **Retrospective Analysis:** A retrospective analysis or retrospective study is a research method that is used when the outcome of an event is already known. If an outcome is known already like a malware infection, retrospective analysis could elp you find the source.

5.0 Incident Handling

Q. 5.1 Classify intrusion events into these categories as defined in the diamond model of intrusion

A1. Items 5.1[a-f] is actually the **Kill Chain** not the **Diamond Model**, but the answers follow.

5.1.a Reconnaissance = research, identification and selection of targets; can use web sites, news articles, social media, gathering of intelligence, address lookup and who is record

5.1.b Weaponization = Couple a remote access Trojan with an exploit into a deliverable, an automated tool (weaponizer); Development of a cyber weapon based on reconnaissance (ie: Viruses, Code injection, Email or phishing campaigns, Exploits for system vulnerabilities, Zero day attacks), attach it to Adobe PDF or Microsoft Office documents

5.1.c Delivery = transmission of the weapon to the targeted environment via communication vector like email attachments, websites, USB removable media; To avoid detection delivery uses obfuscastion, (hidden or not clear data), or encryption so it is unreadable

5.1.d Exploitation = triggers intruders' code, application or operating system vulnerability, users themselves, an operating system feature that auto-executes code, SQL injection, etc.

5.1.e Installation = maintain persistence inside the environment; establish back door to target with no alerts to defenders over a prolonged time, will survive a reboot and avoid malware and virus detection, also can create botnets

5.1.f Command and control = compromised hosts must beacon outbound to an Internet controller or server to establish a CnC channel via DNS, HTTP, HTTPS, and so on. Could be encrypted. Commands are sent to malicious software programs on a server that could eventually impact the entire network, interent relay chat, (IRC) messages are a clue to CnC activity.

5.1.g Action on objectives = data exfiltration, which involves collecting, encrypting, and extracting, violations of data integrity or availability and possible use as a hop point, to compromise additional systems; goals include intellectual property theft, data theft, bandwidth theft/DoS, spam, botnet expansion, etc. It is tough to defeat the threat actor once they have gotten to this point.

A2. The diamond model sets the following characteristics:

Adversary: The threat actor or organization responsible for utilizing a capability against the victim to achieve their intent. The knowledge about the adversary is generally elusive, and this node is likely to be empty for most events, at least at the time of discovery

Capability: The tools and/or techniques of the adversary that are used in the event

Infrastructure: The physical and/or logical communication structures the adversary uses to deliver a capability, maintain control of capabilities (for example, CnC), and effect results from the victim (for example, exfiltrate data)

Victim: The adversary’s target against whom vulnerabilities and exposures are exploited and capabilities are used.

The diamond model is centered per node, but supports analytical **Pivoting** which may start focusing on the **Adversary** but later shift the focus to the **Victim**. The diamond model has Meta Features for the data that include:

Timestamp: When the event occurred, broken into start and end times.

Phase: A group of events, similar to the phases of the kill chain. The diamond model does not assume that there will always be seven phases to an attack.

Result: The post condition of the adversary's operation, which may be Success, Failure, or Unknown.

Direction: Denotes where the event's actions that are started from adversary to victim, victim to

adversary, or infrastructure being an intermediary in either case

Methodology: A generic class of activity like distributed DoS, spear-phishing attacks, etc.

Resources: Software, hardware, or money.

Q. 5.2 Apply the NIST.SP800-61 r2 incident handling process to an event

A. Am not sure how incident handling differs from incident response in section 3 above.

Q. 5.3 Define these activities as they relate to incident handling **A1.**
Items 5.3[a-f] answers follow. Chapter 13: Section 3.

5.3.a **Identification** = The SOC analyst performs continuous monitoring, and active cyber threat hunting. When a true positive incident has been detected, the incident response team is activated. During the investigation process, the SOC analyst or the incident response team may also contact the CERT/CC, or other security intelligence sources, which tracks Internet security activity and has the most current threat information.

5.3.b **Scoping** = **Analysis:** The incident response team should work quickly to analyze and validate each incident, following a pre-defined process and documenting each step that is taken. When the team believes that an incident has occurred, the team should rapidly perform an initial analysis to determine the incident's **Scope**.

The initial analysis may include:

Which networks, systems, or applications are affected?

Who or what originated the incident?

What tools or attack methods are being used?

Which vulnerabilities are being exploited?

The initial analysis should provide enough information for the team to prioritize subsequent activities, such as containment of the incident and deeper analysis of the effects of the incident (if required, this deeper analysis may occur after the containment phase).

5.3.c **Containment** = Incident containment is perhaps the hardest and most important decision that is made during an incident.

Decision points for containment may include:

What is the scope of the incident?

What is the type of advice?

What is the network reachability of the device that has been affected by the incident?

How quickly the incident response team can get containment in place?

How quickly containment is needed?

Last, but not least, is the reality that not all incidents are created equal and neither are containment options. The broader picture must be considered. For example, if data exfiltration is currently taking place, the incident response team may need to move quickly to contain and minimize the damage.

Without taking the time initially to understand each facet of containment, documenting them, testing them, and knowing the available fallback options, it is likely that the incident response team will fumble in making such a critical decision. Also, if the containment's impact on the business is not well understood, containment may do more harm than good.

5.3.d **Remediation** = **Eradication and recovery:** The incident response team investigates to find the origin of the incident. The root cause of the problem and all traces of potentially malicious code are removed, which may also involve changing passwords for accounts, **hardening systems**, and so on. Data and software are restored from clean backup files, ensuring that no vulnerabilities remain. After recovery, the systems are monitored for any sign of weakness and incident recurrence. Recovery may also involve tactical fixes including user account changes, patching software, and **device hardening**, and prioritizing strategic fixes such as process changes.
5.3.e **Lesson-based hardening** = **Lessons learned:** The incident response team analyzes how and why the incident happened and performs an FMEA, (failure modes and effects analysis), against it. FMEA is a qualitative and systematic tool, usually created within a spreadsheet, to help practitioners anticipate what might go wrong with a product or process. This phase includes documenting how the incident was handled, recommendations for better future response, and how to prevent a recurrence.

5.3.f **Reporting** = Incident response plan should include provisions concerning incident **reporting**. The reporting should also be immediate and occur at pre-defined intervals which are based on the incident severity. When an incident is analyzed and prioritized, the incident response team needs to notify the appropriate individuals so that all who need to be involved will play their roles. Reporting can be both internal and external teams. Exact reporting requirements vary among organizations, but parties that are typically notified include the CIO, the head of information security, the system owner, HR, public affairs, the legal department, and law enforcement. Organizations that are trying to share information with external organizations should also consult with their legal department before initiating any coordination efforts. Contracts or other agreements may need to be put into place before external discussions occur. An example is an NDA to protect the confidentiality of the organization's most sensitive information.

Q. 5.4 Describe these concepts as they are documented in NIST SP800-86
5.4.a **Evidence collection order** = Data acquisition should be performed using a three-step process: developing a plan to acquire the data, acquiring the data, and verifying the integrity of the acquired data:

1. Developing a plan is an important first step in most cases because there are multiple potential data sources. The analyst should create a plan that prioritizes the sources, establishing the order in which the data should be acquired.

2. If the data has not already been acquired by security tools, analysis tools, orother means, the general process for acquiring data involves using forensic tools to collect volatile data, duplicating non-volatile data sources to collect their data, and securing the original non-volatile data sources. Data acquisition can be performed either locally or over a network. Although it is generally preferable to acquire data locally because there is greater control over the system and data, local data collection is not always feasible

3. After the data has been acquired, its integrity should beverified. It is particularly important for an analyst to prove that the data has not been tampered with if it might be needed for legal reasons. Data integrity verification typically consists of using tools to compute the message digest of the original and copied data, then comparing the digests to make sure that they are the same.

5.4.b **Data integrity** = Data File Integrity: During backups and imaging, the integrity of the original media should be maintained. To ensure that the backup or imaging process does not alter data on the original media, analysts can use a write-blocker while backing up or imaging the media. A write-blocker is a hardware or software-based tool that prevents a computer from writing to computer storage media connected to it. Hardware write-blockers are physically connected to the computer and the storage media being processed to prevent any writes to the disk. After a backup or imaging is performed, it is important to verify that the copied data is an exact duplicate of the original data. Computing the message digest of the copied data can be used to verify and ensure data integrity. A message digest is a hash that uniquely identifies data and has the property that changing a single bit in the data will cause a completely different message digest to be generated. There are many algorithms for computing the message digest of data, but the two most commonly used are MD5 and Secure Hash Algorithm 1, SHA-1.

5.4.c **Data preservation** = If an analyst needs to establish an accurate timeline of events, then the file times should be preserved. Accordingly, analysts should be aware that not all methods for collecting data files can preserve file times. Bit stream images can preserve file times because a bit-for-bit copy is generated; performing a logical backup using some tools may cause file creation times to be altered when the data file is copied. For this reason, whenever file times are essential, bit stream imaging should be used to collect data. Analysts should also be aware that file times may not always be accurate. Among the reasons for such inaccuracies are the following:

1. The computer's clock does not have the correct time. For example, the clock may not have been synchronized regularly with an authoritative time source.

2. The time may not be recorded with the expected level of detail, such omitting the seconds orminutes.

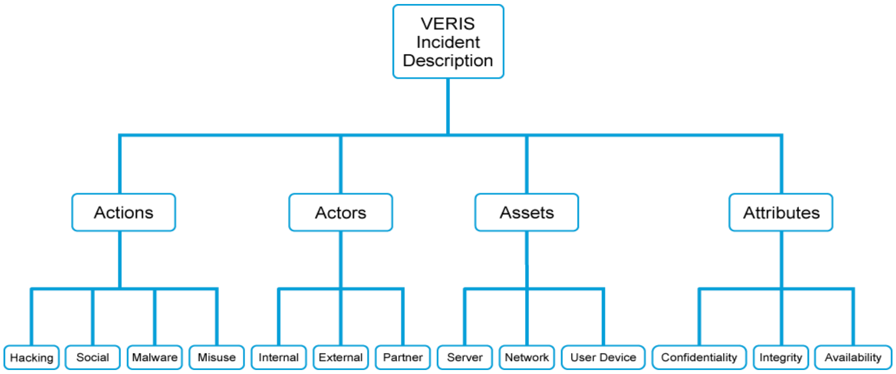
3. An attacker may have altered the recorded file times.

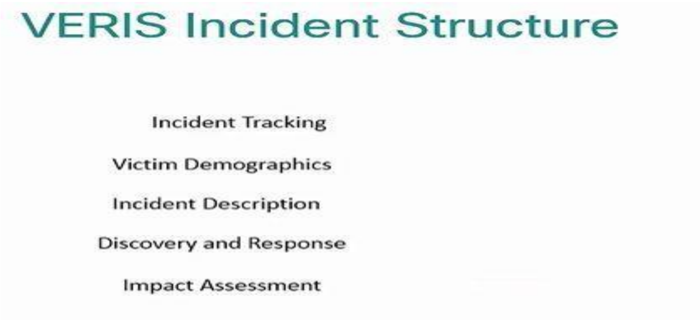
Before the analyst begins to collect any data, a decision should be made by the analyst or management (in accordance with the organization's policies and legal advisors) on the need to collect and preserve evidence in a way that supports its use in future legal or internal disciplinary proceedings. In such situations, a clearly defined chain of custody should be followed to avoid allegations of mishandling or tampering of evidence. This involves keeping a log of every person who had physical custody of the evidence, documenting the actions that they performed on the evidence and at what time, storing the evidence in a secure location when it is not being used, making a copy of the evidence and performing examination and analysis using only the copied evidence, and verifying the integrity of the original and copied evidence. If it is unclear whether or not evidence needs to be preserved, by default it generally should be preserved.

5.4.d **Volatile data collection** = Volatile data refers to data on a live system that is lost after a computer is powered down, such as the current network connections to and from the system. Volatile OS data should be collected before the computer is powered down. OSs execute within the RAM of a system. While the OS is functioning, the contents of RAM are constantly changing. At any given time, RAM might contain many types of data and information that cou09uj ld be of interest. For example, RAM often contains frequently and recently accessed data, such as data files, password hashes, and recent commands. In addition, like filesystems, RAM can contain residual data in slack, free space, network configuration, network connections, running processes, open files, login sessions, and operating system time.

Q. 5.5 Apply the VERIS schema categories to a given incident

A. The figure shows the four main VERIS components (actors, actions, assets, and attributes, which are known as the 4 A's) that are used to describe an incident. The items at the bottom are the issues with each A.




VERIS Incident Structure

Incident Tracking

Victim Demographics

Incident Description

Discovery and Response

Impact Assessment

incident tracking section captures general information about the incident. The main purpose is allowing organizations to identify, store, and retrieve incidents over time.

victim demographics section describes (but does not identify) the organization that is affected by the incident. The primary purpose is to aid comparisons between different types of organizations (across industries, sizes, regions, and so on) or departments within a single organization.

incident description section translates the incident narrative of “who did what to what (or whom) with what result” into a form that is more suitable for trending and analysis.

discovery and response section focuses on the timeline of the events, how the incident was discovered, and lessons learned during the response and remediation process. It provides useful insight into the detection and defensive capabilities of the organization and helps identify corrective actions that are needed to detect and prevent similar incidents in the future

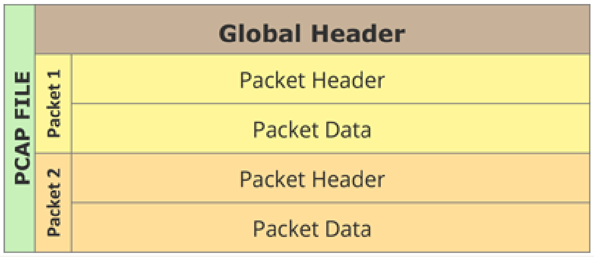
impact assessment section leverages three perspectives of the impact in order to provide an understanding and measure of consequence that is associated with the incident. Together, they seek to categorize the varieties of losses that are experienced, estimate their magnitude, and capture a qualitative assessment of the overall effect on the organization

Other general things to know for the exam. **Q.**

What is a Libpcap file?

A. Libpcap File Format

The libpcap file format is the main capture file format used in TcpDump/WinDump, Snort, and many other networking tools. It is fully supported by Wireshark/TShark, but they now generate pcapng files by default.



The Global Header contains among other metadata, the time zone indicator “**thiszone**”, which by default is always set to **0** to indicate **GMT (UTC)**. Theoretically, this value can be set as UTC +10 – for example for Sydney, Australia. In this case the value of “thiszone” will be -36000. In practice, however, time stamps are always stored in GMT (UTC) format.

Q. What are the four basic phases of the forensic process?

A. The four basic phases are the following:

Collection: The first phase in the process is to identify, label, record, and acquire data from the possible sources of relevant data, while following guidelines and procedures that preserve the integrity of the data.

Examination: Examinations involve forensically processing large amounts of collected data using a combination of automated and manual methods to assess and extract data of particular interest, while preserving the integrity of the data.

Analysis: The next phase of the process is to analyze the results of the examination, using legally justifiable methods and techniques, to derive useful information that addresses the questions that were the impetus for performing the collection and examination.

Reporting: The final phase is reporting the results of the analysis, which may include describing the actions used, explaining the tools, determining what other actions need to be performed, securing identified vulnerabilities, and improving existing security controls.