Incident Response & Forensics

Well, an incident response is a set of procedures that an investigator follows when they're examining a computer security incident. These incident response procedures are part of your organization's overall computer security incident management program. This program should consist of the monitoring and detection of security events on a computer network and the execution of proper responses to those security events. Now, every organization has their own way of doing incident response.
But a basic six-step procedure looks something like this:

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons learned.

For the exam, you want to know these six steps and you want to know the right order.

Incident Response Planning

IR Team

Well, your incident response team is key people that are going to be available to respond to any incident that meets the severity and priority thresholds that are set out by your incident response plan, because not everything that you run into is going to require you to activate your incident response team. Some things can just be handled by your incident handlers and you don't need the full team to do it. But if you have a big issue, like an ongoing data breach or something like that, you're going to want the entire incident response team. So, what type of positions are on this incident response team?

Well, first, you're going to have an **incident response manager or team lead**, this

person is going to oversee and prioritize actions during the detection, analysis, and containment of an incident. This is a position that I have personally filled numerous times. And I can tell you, it is a difficult position that requires a lot of good soft skills in addition to those traditional in-depth technical skills that some other positions are going to require.

The second position we have is a **security analyst**. Your team needs to have one or more security analysts assigned in order to work directly on the affected network and to play detective in order to determine what happened up to this point. Your security analyst may be assigned into two categories, although some analysts may be working in both categories simultaneously when dealing with a smaller-scale incident. The first of these is known as a triage analyst. A triage analyst is a security analyst that's assigned to work on the network during the incident response. Triage analysts are going to help filter out false positives by properly configuring intrusion detection and protection systems, as well as performing ongoing monitoring and analysis to detect any new or potential intrusions during your incident response. Another type of security analysts we use is what's known as a forensic analyst. Now, a forensic analyst, on the other hand, is going to be more focused on the detective work and trying to piece together what has already occurred on the network. They're going to focus on recovering key artifacts and evidence from the network and then use these to build a timeline of the different events that led up to the incident itself and that way, we can understand what happened up to this point.

Beyond that, you're also going to want to have a **threat researcher**, this is another key part of your team. These threat researchers are able to complement your analysts by providing threat intelligence and overall context during your incident response. These specialists work to always remain up-to-date on the current threats that are facing your organization and your specific industry, as well as keeping up-to-date with previous incidents that may have occurred. I like to think about these folks as both a combination of a futurist in terms of guessing what the bad guys might do, as well as a historian because they know all the bad things that the bad guys have done in the past.

Finally, we have **cross functional support**. In addition to all the critical roles I already talked about, we also want to expand our team with additional cross functional support. This includes people from management or the executive team, somebody from human resources, if you're dealing with an employee insider threat, or an attorney or lawyer in the case that the company may want to take legal action against the perpetrator or the attacker.

Now, this incident response team is often known as a **CSIRT**. A CSIRT is the computer security incident response team, and your CSIRT should be the single point of contact for security incidents. Now, the CSIRT may be part of the SOC, the Security Operations Center, or they could be an independent team. It just depends on how your organization has set this up. In fact, some organizations have chosen to outsource their security response and their CSIRT teams. This way, whenever there's an incident, they would call on this third-party contractor who will bring their experts to help you bring your systems back online and get the bad guys out of your network.

When you have an incident, you need to start thinking about who are the affected stakeholders? There are lots of them out there, inside and outside your organization.

Senior Leadership

When we talk about senior leadership, this is the executives and managers who are responsible for business operations and various functional areas within your company. Now, the reason this is important is because a lot of our incident responders tend to be technical people. And so, we might, as technical people say, the quickest way to solve this incident is to shut down that server. But if we're not understanding the business impact to those actions, that could have second and third-order effects that'd be very bad for our organization. So, we're going to have to get senior leadership involved to understand if I do this, it's going to have this and that and the other effect, and we have to mitigate those.

Regulatory Bodies

The next key stakeholder we have to consider is regulatory bodies. These are governmental organizations that oversee the compliance with specific regulations and laws. For example, if we're talking about HIPAA, which has to do with health care, you're going to have to be overseen by Health and Human Services, because they're the ones who run the HIPAA program.

Legal

The next stakeholder we have to consider is legal. Now, legal is the business or organization's legal counsel, and they're going to be responsible for mitigating risk from civil lawsuits. For example, as you're planning out your response of what you're going to do to stop the breach of data, you want to make sure legal is in the room

because your actions could come up later on if your company is sued for its response.

Law Enforcement

On the other side of the coin, we have law enforcement, and law enforcement is an external stakeholder, they may provide services to assist in your incident into handling efforts, or to prepare for legal action against the attacker in the future. Now, one quick thing to note, your decision to involve law enforcement has to be made by senior executives with guidance from your internal legal counsel. You, as an incident responder, should not immediately pick up the phone and call the FBI or the local police. This is something your business has to decide. Now, there are cases where it is legally required to bring in law enforcement. But in a lot of cases, it is more of a civil issue. And you have the determination and the right to decide if you want to press charges and bring in law enforcement. So, keep that in mind. And remember, your senior executives get to make that decision.

HR

Our next stakeholder is human resources, and this is an internal stakeholder. They're going to be used to ensure there's no breaches of employment law or employee contracts during the incident response. For example, if you're a suspecting that there's an internal threat, and you start questioning employees, or you want to start going through employee files, you're going to have to consult human resources, because you could be breaching employment law or employee contracts, so, make sure you involve human resources.

PR

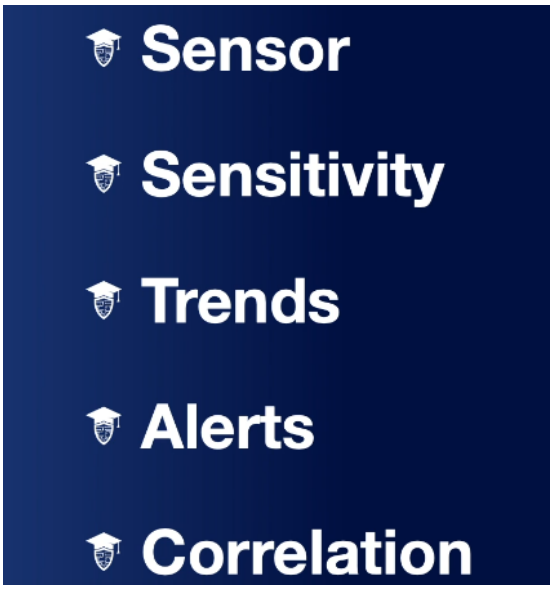
Public relations is used to manage the negative publicity from a serious incident. Now, this is important because you want to make sure, as the technical lead, as an incident responder, you're not the one answering questions to the media. You don't want to be the one up there behind all those microphones with a sea of reporters asking you questions. You have people in your organization whose job it is to handle that. And they're going to come up with a clear, concise message that can be said over and over again to all the inquiries reporters have.

Investigative Data

SIEM

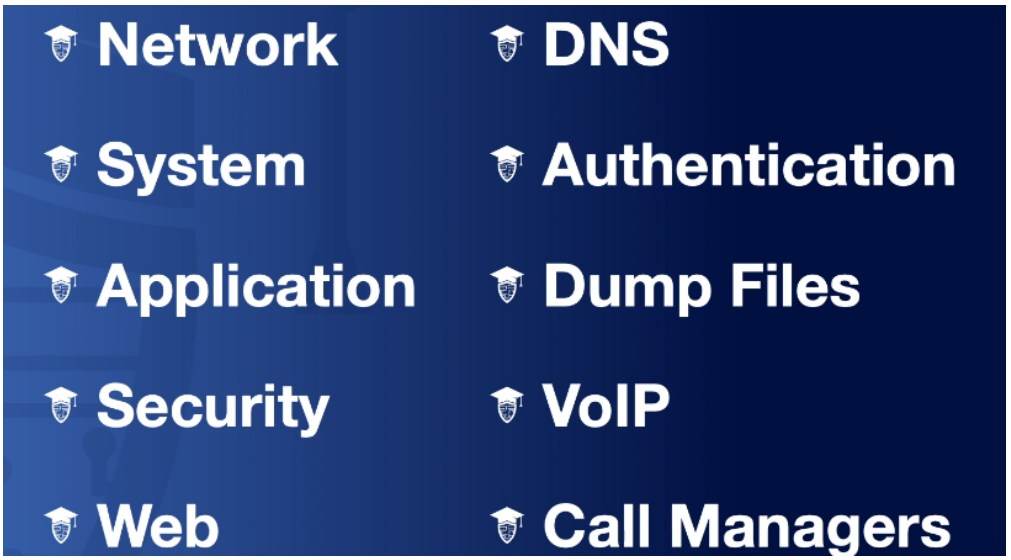
Now, the first thing we're going to talk about is a SIEM. Now, we've talked about SIEMs before, but a SIEM is a Security Information and Event Monitoring System. Now, this is important because it's going to be a combination of a lot of different data sources into this one SIEM tool. And this provides us with real-time analysis of security alerts that are generated by applications and network hardware.

The first thing we have to think about is our sensor. This is the actual end point that's being monitored. That sensor can then feed that data up into the SIEM. Another thing we have to think about with our SIEMs is their sensitivity. Now, the sensitivity is focused on how much or how little you're going to be logging. Based on how you configure that sensor, that's going to determine how much data is being sent to the SIEM. Now, you may think it's great to send everything to the SIEM and in a lot of cases, it is, but you have to remember that a SIEM can become overloaded with too much information. Another thing we have to think about is trends. By using a SIEM and its graphical ability to look across these logs, we can start seeing trends in our network. We might say that every time there is five failed login attempts, I want to have an alert sent to a system administrator to look into that account. That would be an example of an alert based on different inputs across the SIEM. And then, finally, correlation. This is one of the big things within a SIEM because we're getting data from all sorts of different sources across all different types of hosts and network devices. All these things need to be correlated so that we have a good picture of what is really happening.



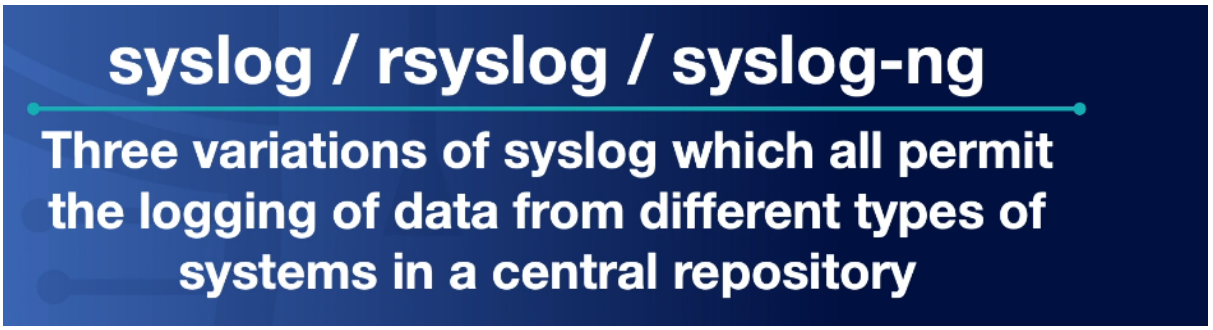
Log Files

We have web log files, and this might be like your proxy server logs, where we could see what websites have been accessed by your users, or if you're running a web server, what files are being touched by an outsider as they're accessing that server.



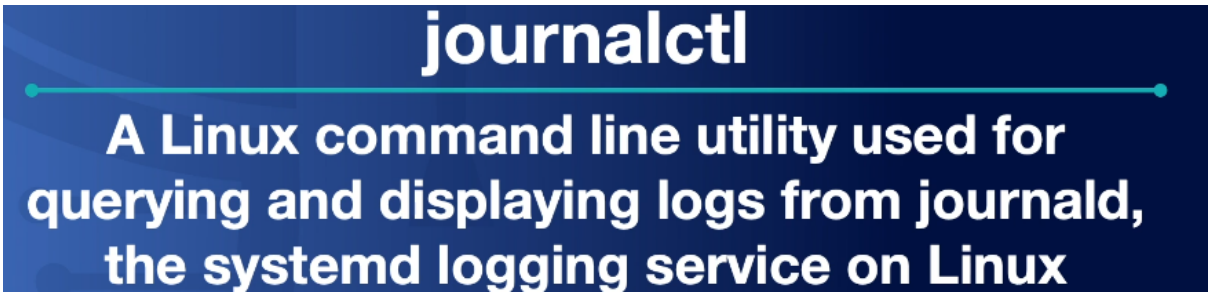
Syslog

Now, the next thing we want to talk about is syslog, rsyslog, and syslog-ng. Now, all three of these are basically three variations that do the same thing. They all are going to permit logging of data from different types of systems into a central repository. One of the things our SIEM relies heavily on is using syslog or rsyslog or syslog-ng to grab that information from all the various end points and dump it into our SIEM.



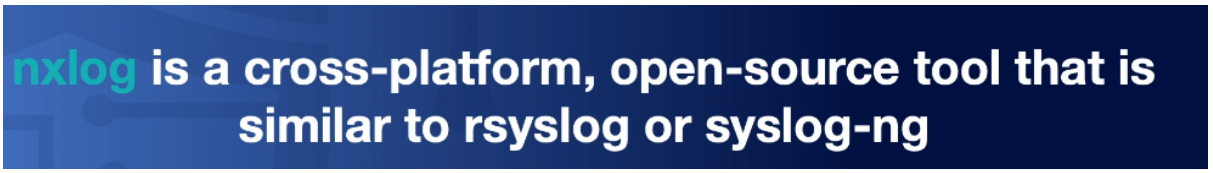
Journalctl

The next tool we want to talk about is journalctl. And this is actually a Linux command line utility that's used for querying and displaying logs from the journald, which is the journal daemon, which is basically, the logging service for systemd on a Linux machine. And so, if you want to be able to look at the logs on a Linux machine, you can use journalctl to do it.



Nxlog

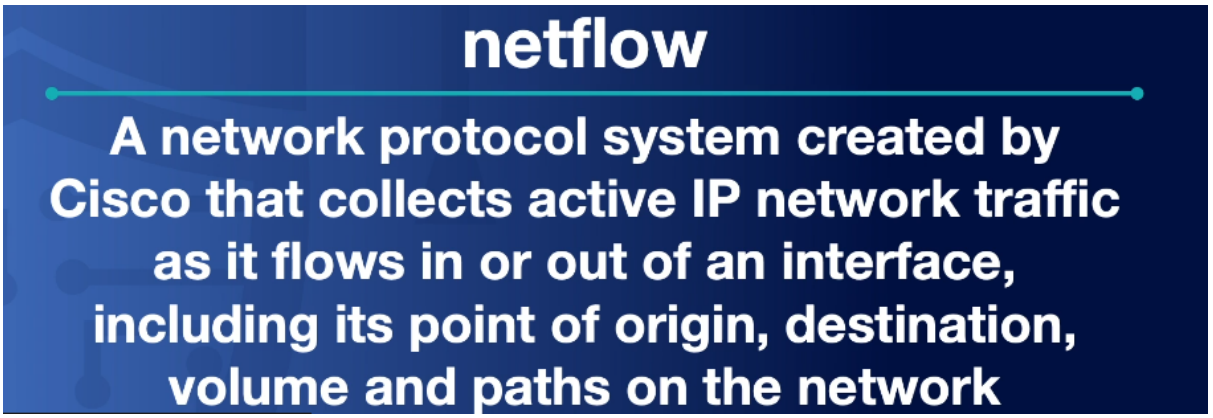
Now, this is a multi-platform log management tool that helps us to easily identify security risks, policy breaches, or analyze operational problems and server logs, operational system logs, and application logs. Now, when you think about nxlog, I want you to remember that it is a multi-platform or cross-platform tool, and it's also open source. This also means that it has a lot of similarities with our syslog or syslog-ng. So, what's the difference? Well, rsyslog and syslog-ng only work on Linux and Unix systems, but nxlog is cross-platform. So, you can use on Unix, Linux, and Windows, too.



Netflow

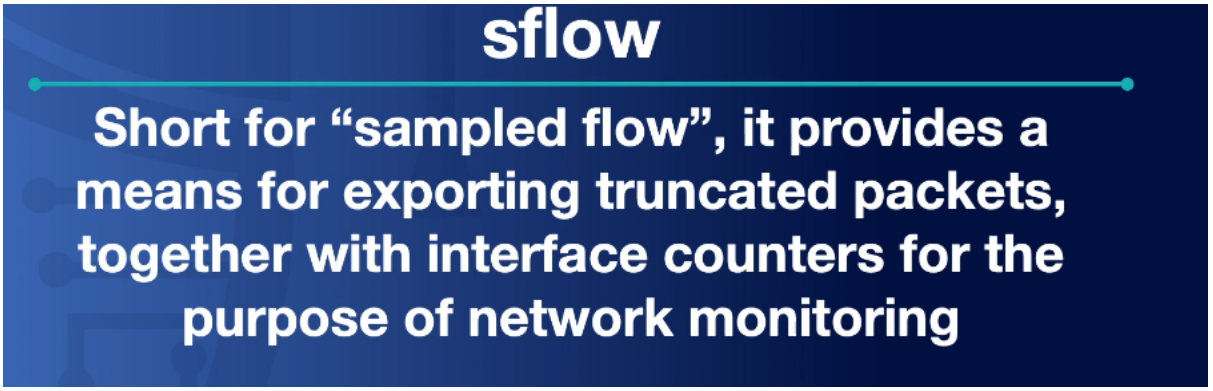
Now, netflow is used in networking and it's a network protocol system that was created by Cisco. And it's going to collect active IP network traffic as it's flowing into or out of an interface. So, as you start thinking about things going into or out of your network, through the firewall or through a router, netflow can actually capture that information. Now, some of the information it captures is things like the point of origin, the destination, the volume, and the paths on the network. This is not a packet capture. We're not capturing everything, every single one and zero that is going in or

out of our network. Instead, netflow is more of a summarization of that data that's going in and out of our network.



Sflow

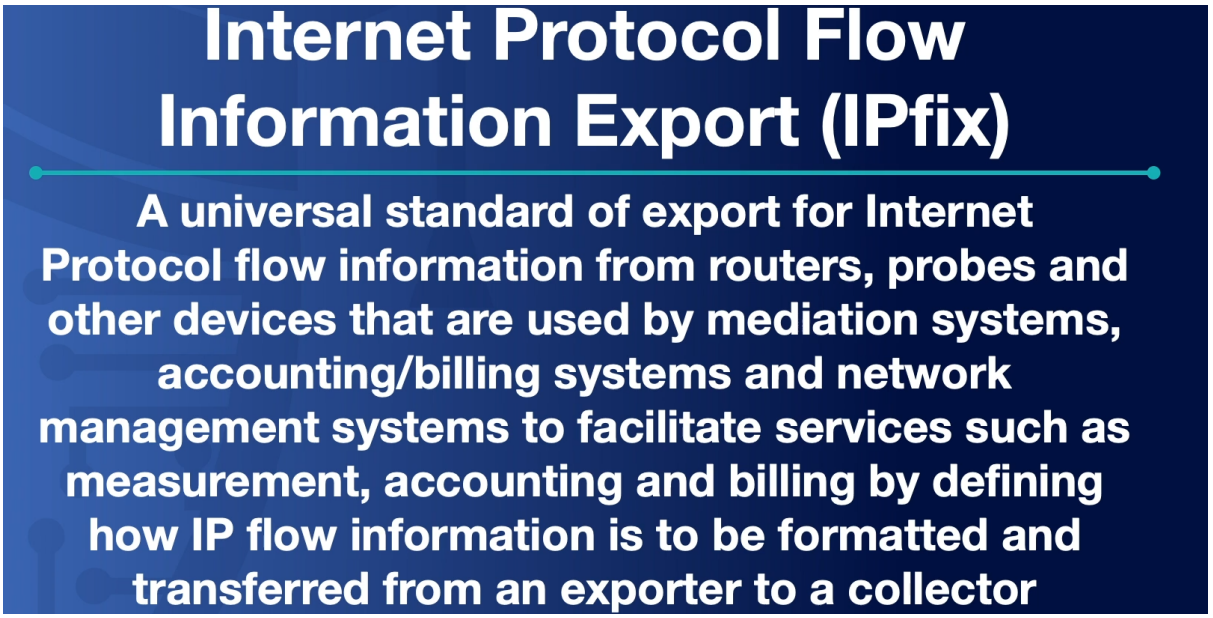
And this stands for Sampled Flow. Essentially, this was an open source version of netflow, where netflow is made by Cisco and it's proprietary, sflow was more of the generic version. It's to provide a means for exporting truncated packets, as well as having an interface counter that is going to be used for network monitoring



IPfix

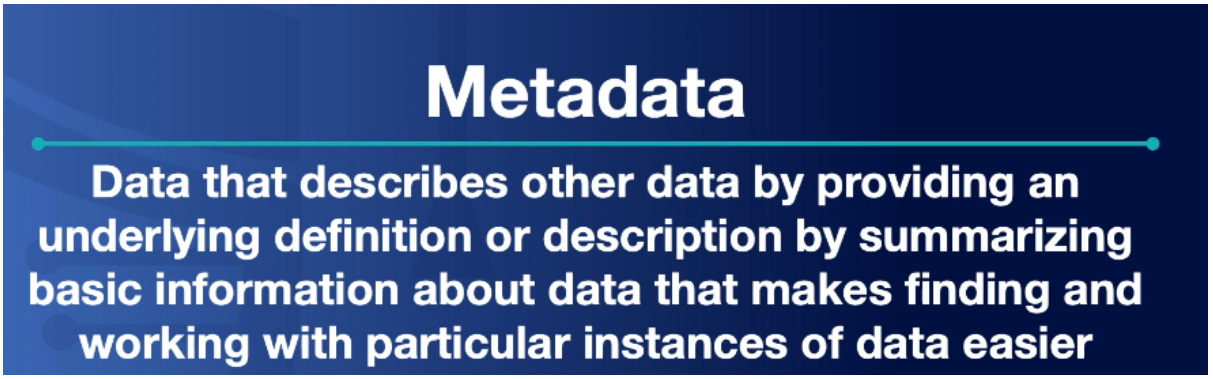
The next thing we have is IPfix, which is the Internet protocol flow information export. Now, this is a universal standard for the export of Internet protocol flow information from your routers, your probes, and other devices that's going to be used by mediation systems, accounting and billing systems, and network management systems to facilitate services such as measurement, accounting, and billing by defining how IP flow information is to be formatted and transferred from an exporter

to a collector. Wow, that is a mouthful. And you may be wondering, what did I just say? Well, really, what IPfix is used for is on the back end of service management.



Metadata

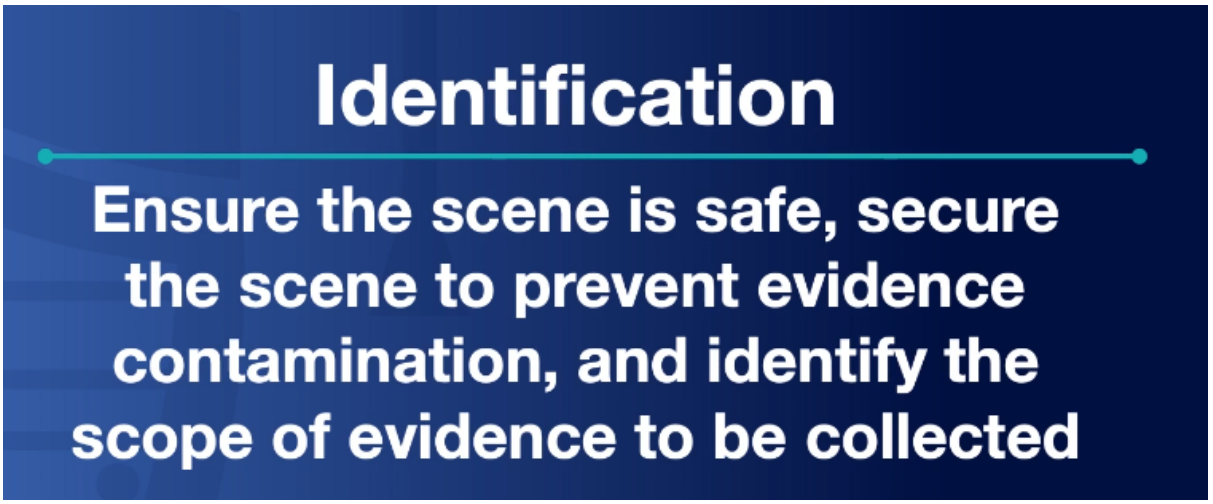
Metadata is going to be data that describes other data, basically, by providing an underlying definition or description by summarizing basic information about the data that makes finding and working with particular instances of data, much easier.



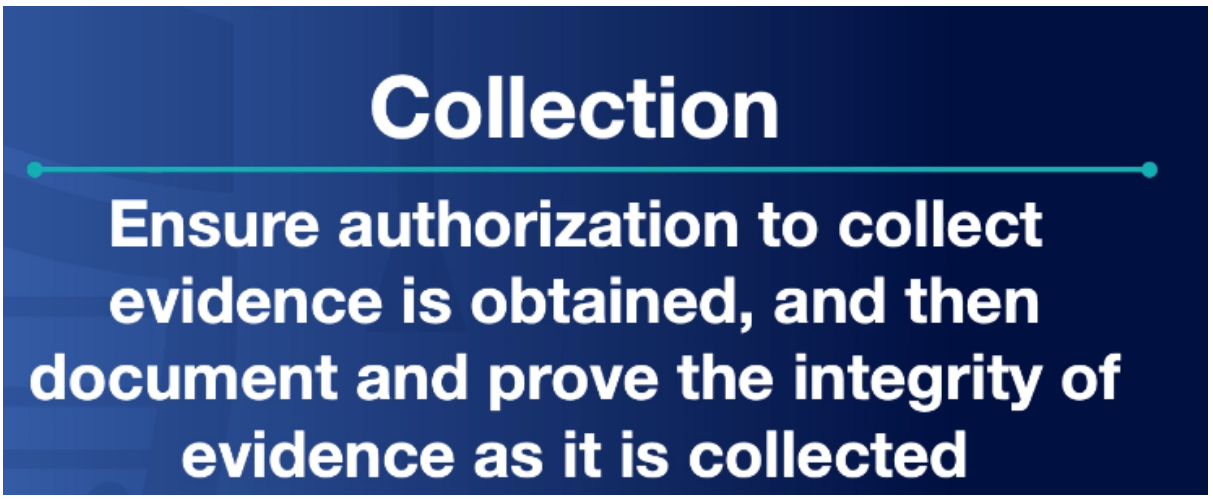
Forensic Procedures

Now, the first thing you need to know about forensics is everything we do we use written procedures. These written procedures are going to ensure that personnel handle forensics properly, effectively, and in compliance with the required regulations. This way, we always follow what is written down and we always do it the same way. Now, as we go through our forensic procedures, there are four main areas. We have identification, collection, analysis, and reporting.

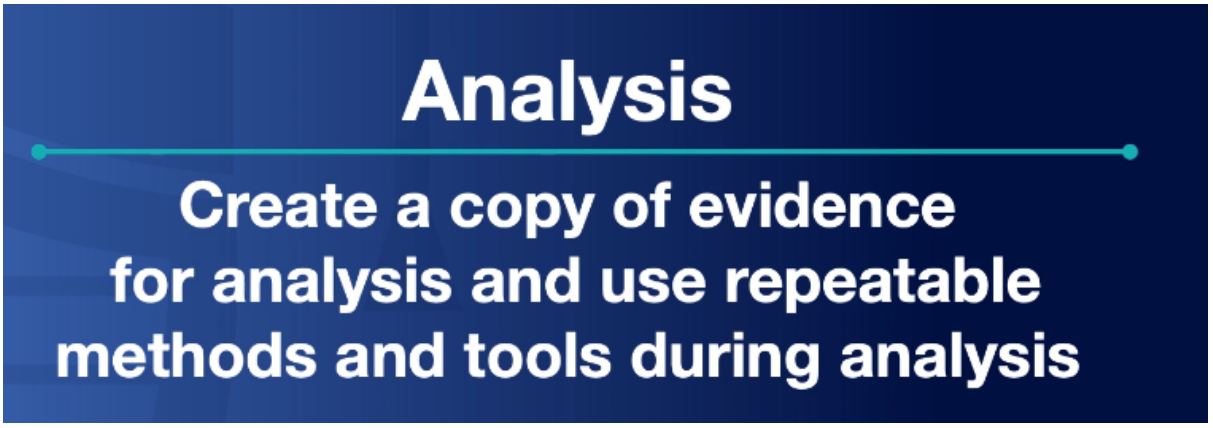
1-Identification



2-Collection



3-Analysis



4-Reporting

Legal Hold

Ethics


1
Analysis must be performed without bias
2
Analysis methods must be repeatable by third parties
3
Evidence must not be changed or manipulated

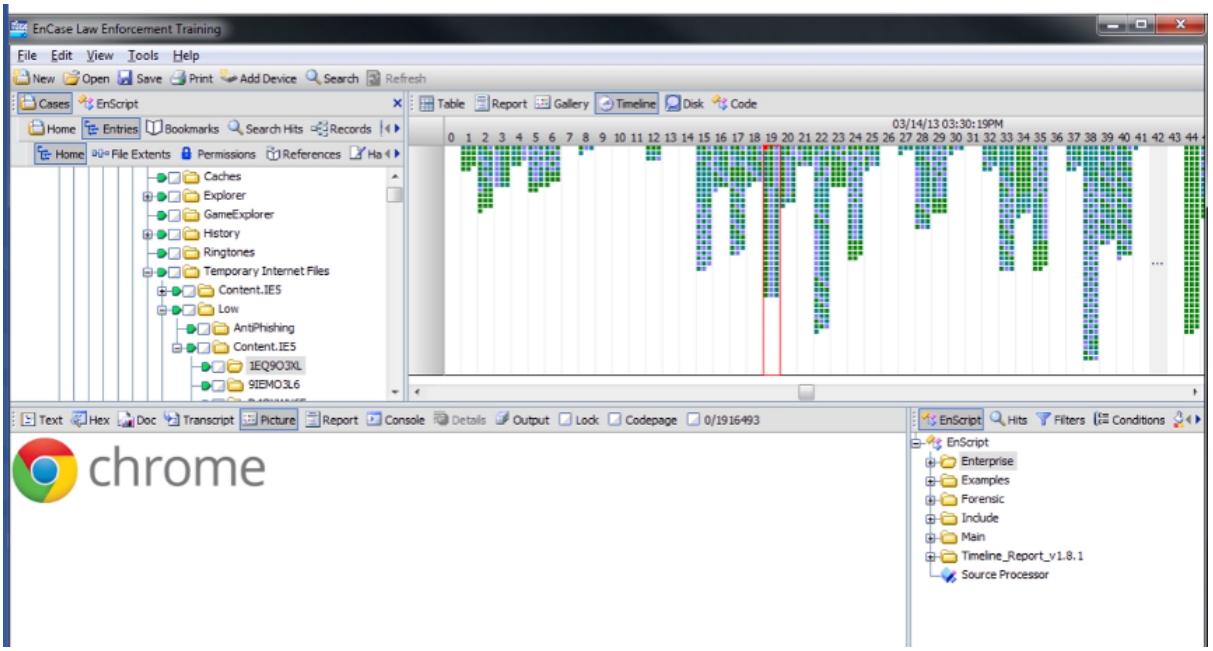
WARNING

Defense attorneys will try to use any deviation from these ethics as a reason to dismiss your findings and analysis

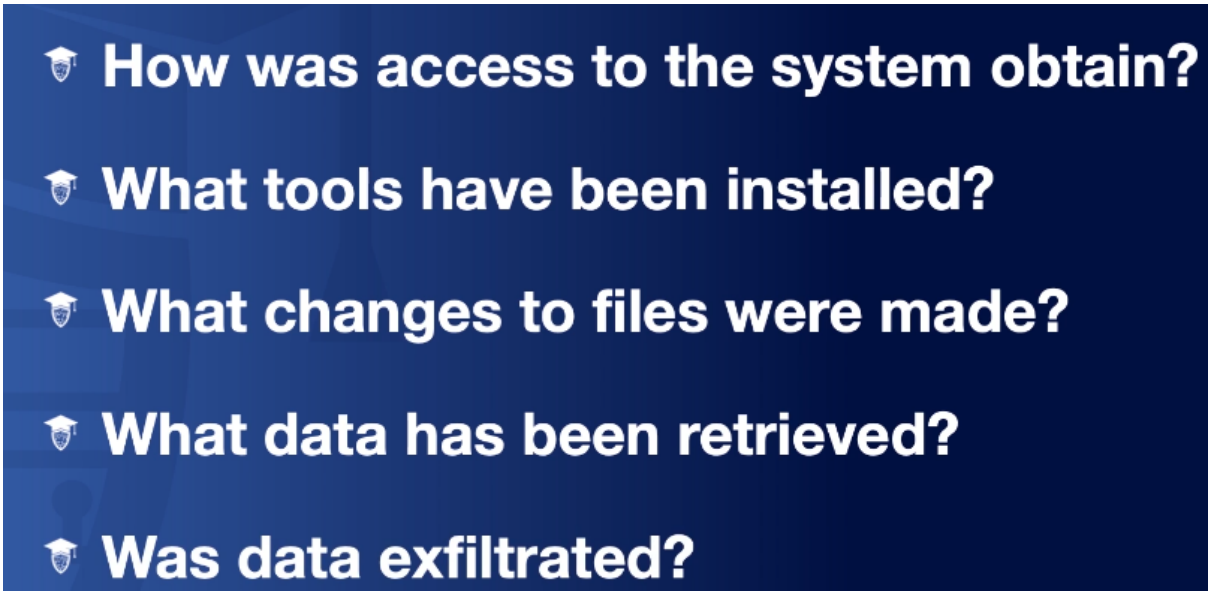
Timeline

Timeline

A tool that shows the sequence of file system events within a source image in a graphical format



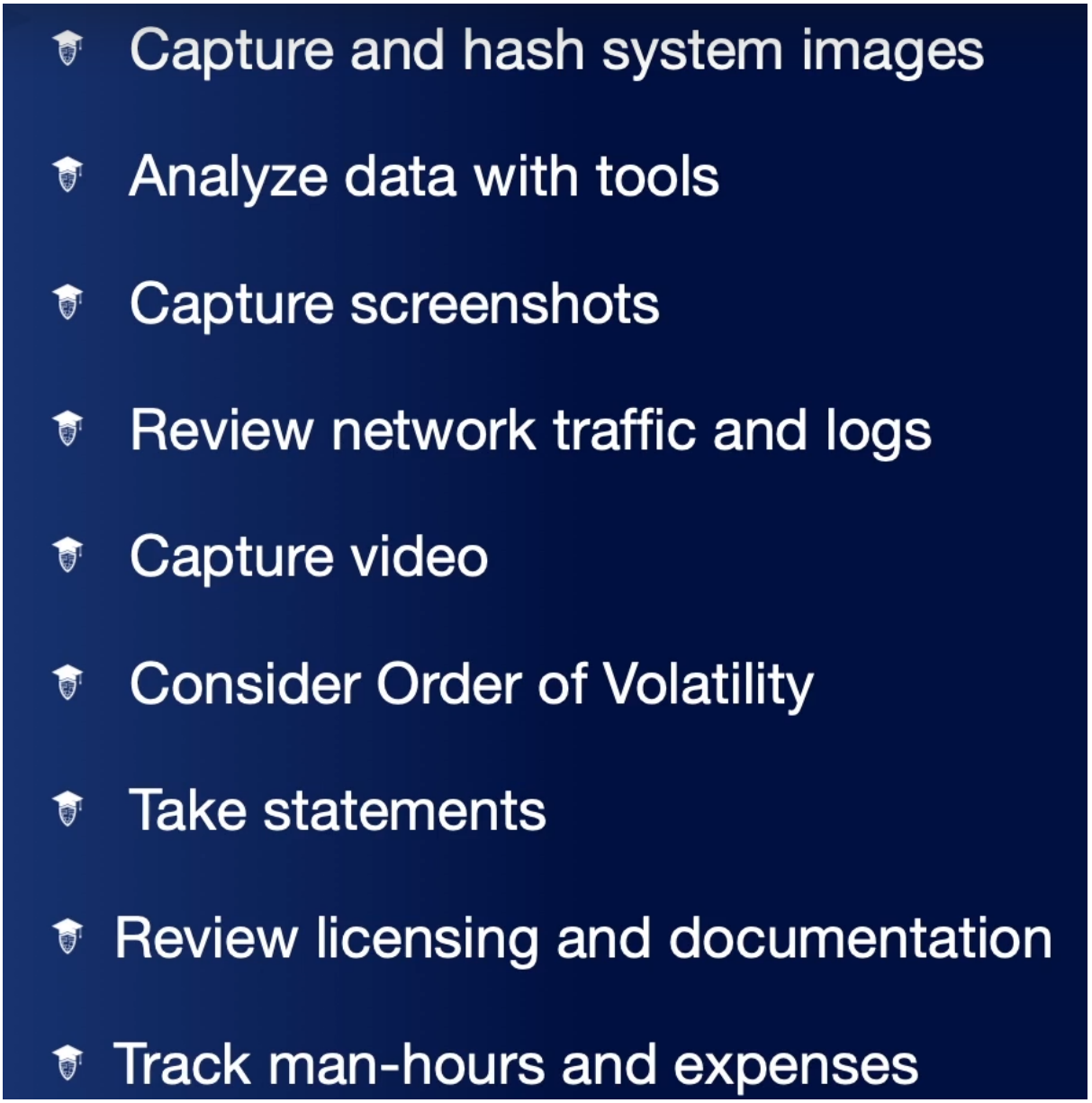
Analysis



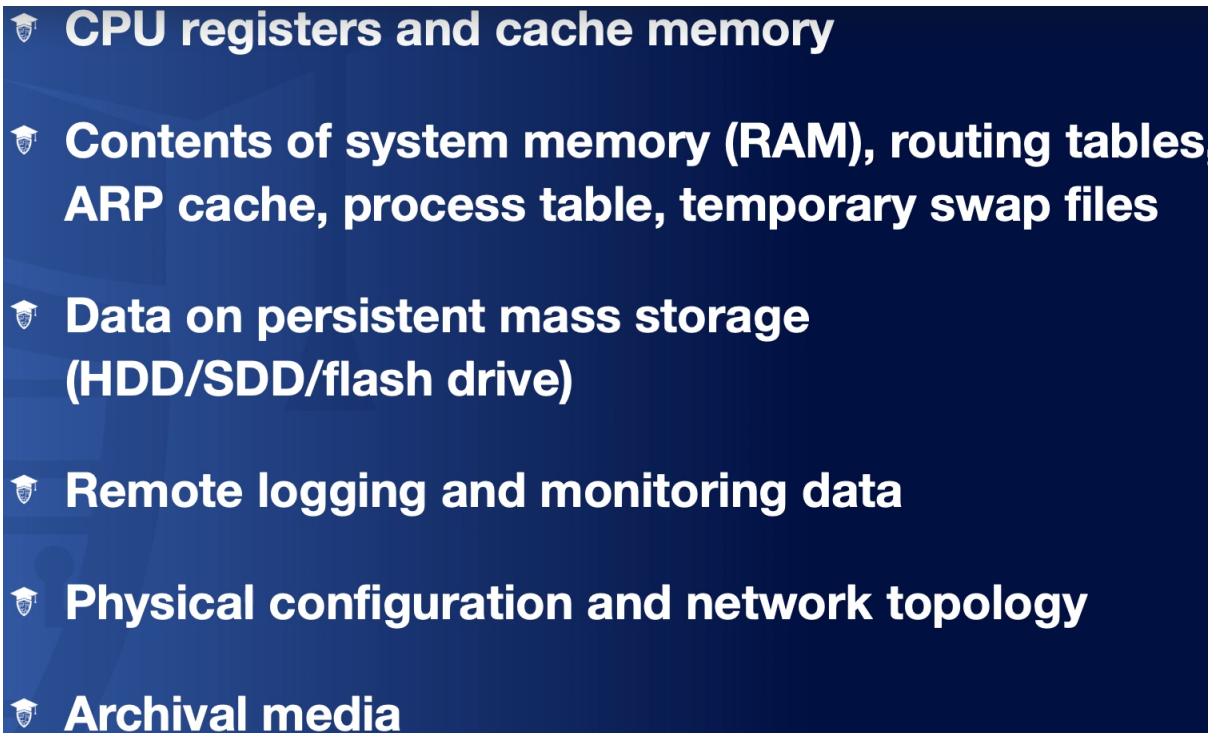
Tools

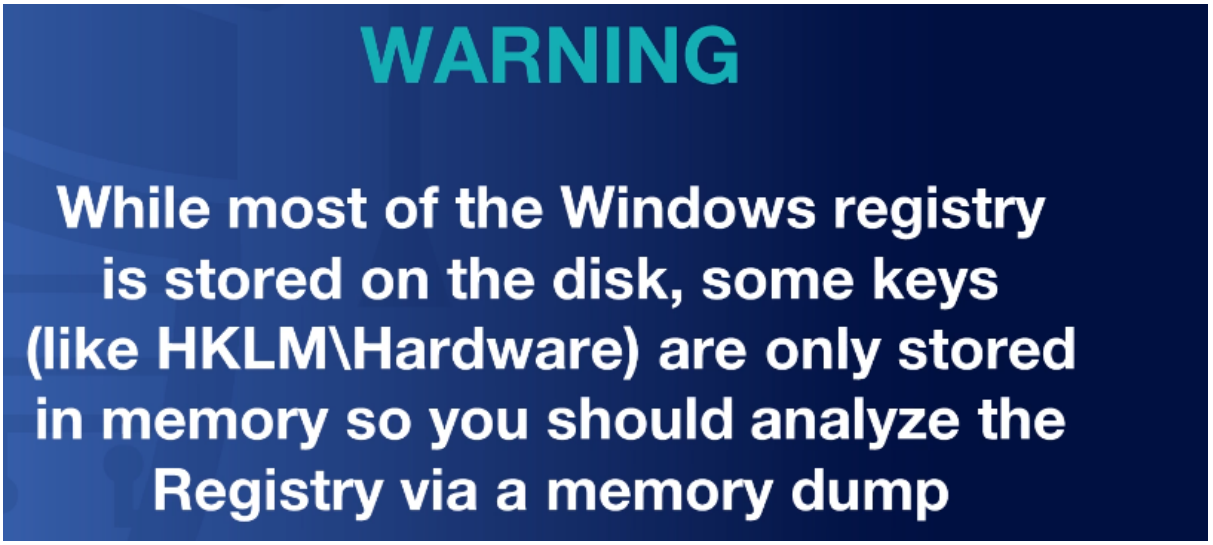
- EnCase
- Autopsy

Data Collection Procedures



For the Security+ exam, no one is going to ask you to conduct this operation, but it's going to give you a taste of digital forensics and see if the idea of being a digital forensics examiner interests you. If it does, you may want to download and play with some forensic tools like **Forensic Toolkit** that I'm going to use in the next lesson or **EnCase**.

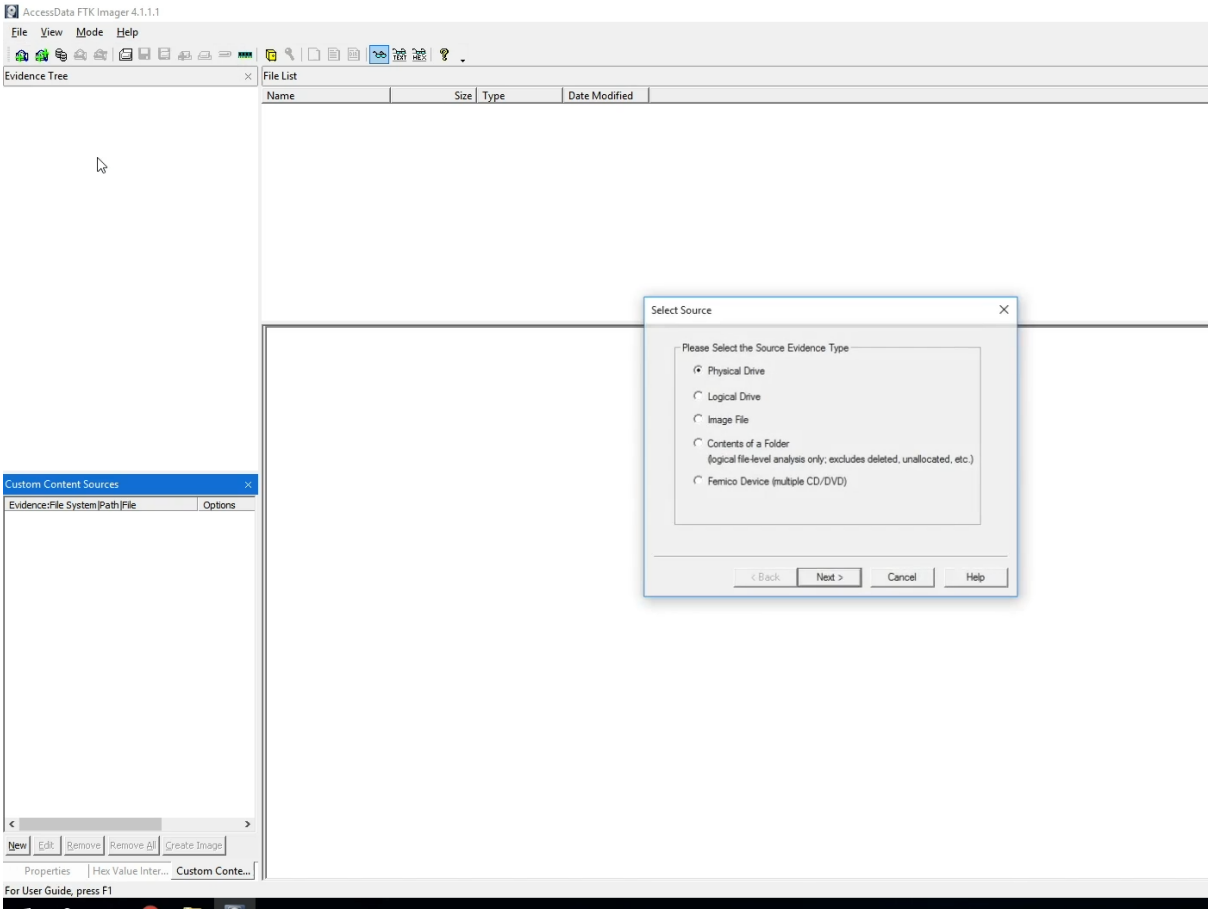


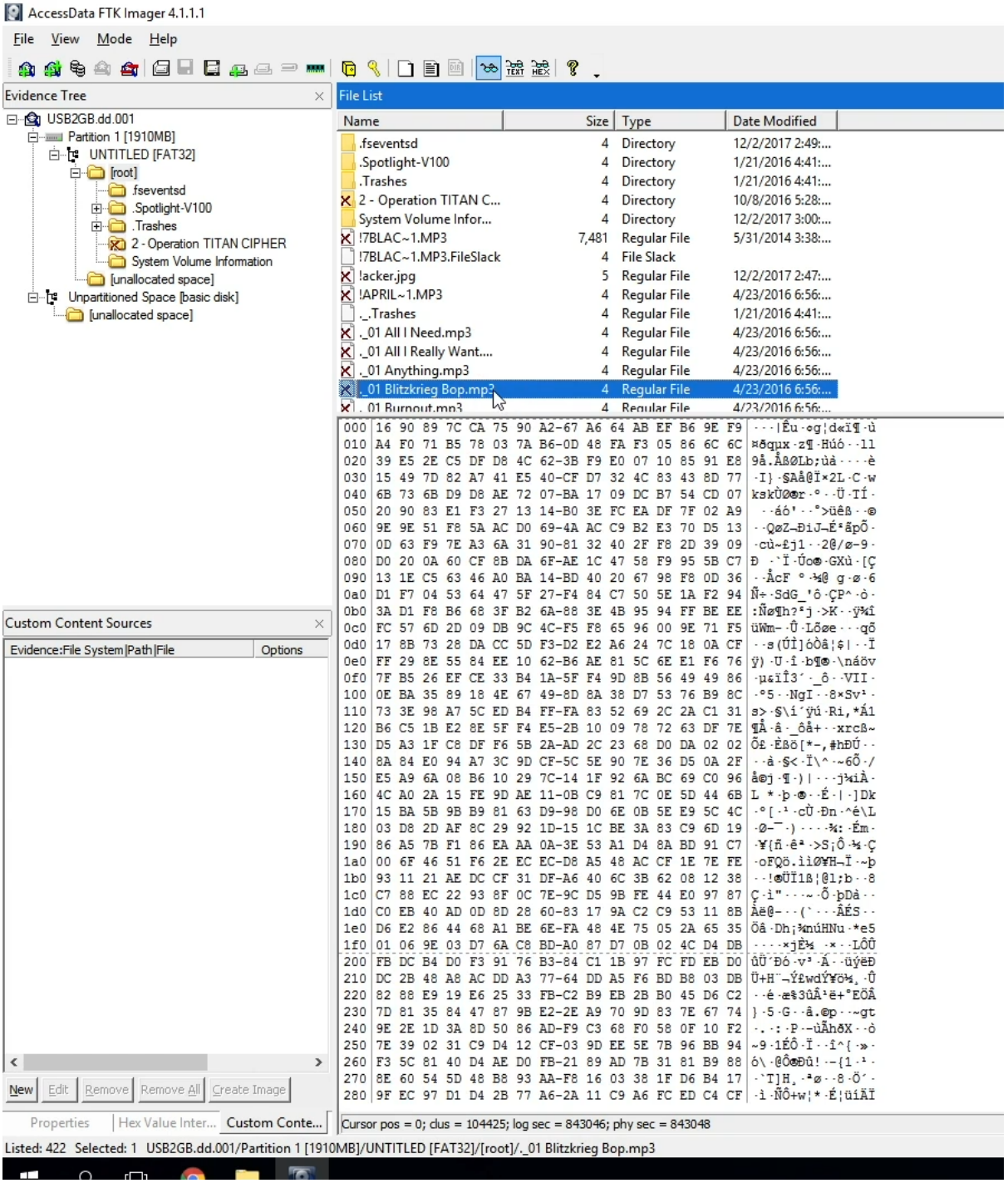


Demo: Disk Imaging

Now, I'm going to show you how we can do this using the Forensic Toolkit Imager or FTK Imager to take a disk image of a hard drive or a USB thumb drive. In my example, I'm going to take a disk image of a 2 GB thumb drive with a Windows machine and then, I'm going to show you a very basic introduction to the Forensic Toolkit or FTK Tool that'll allow you to do a forensic investigation and find deleted

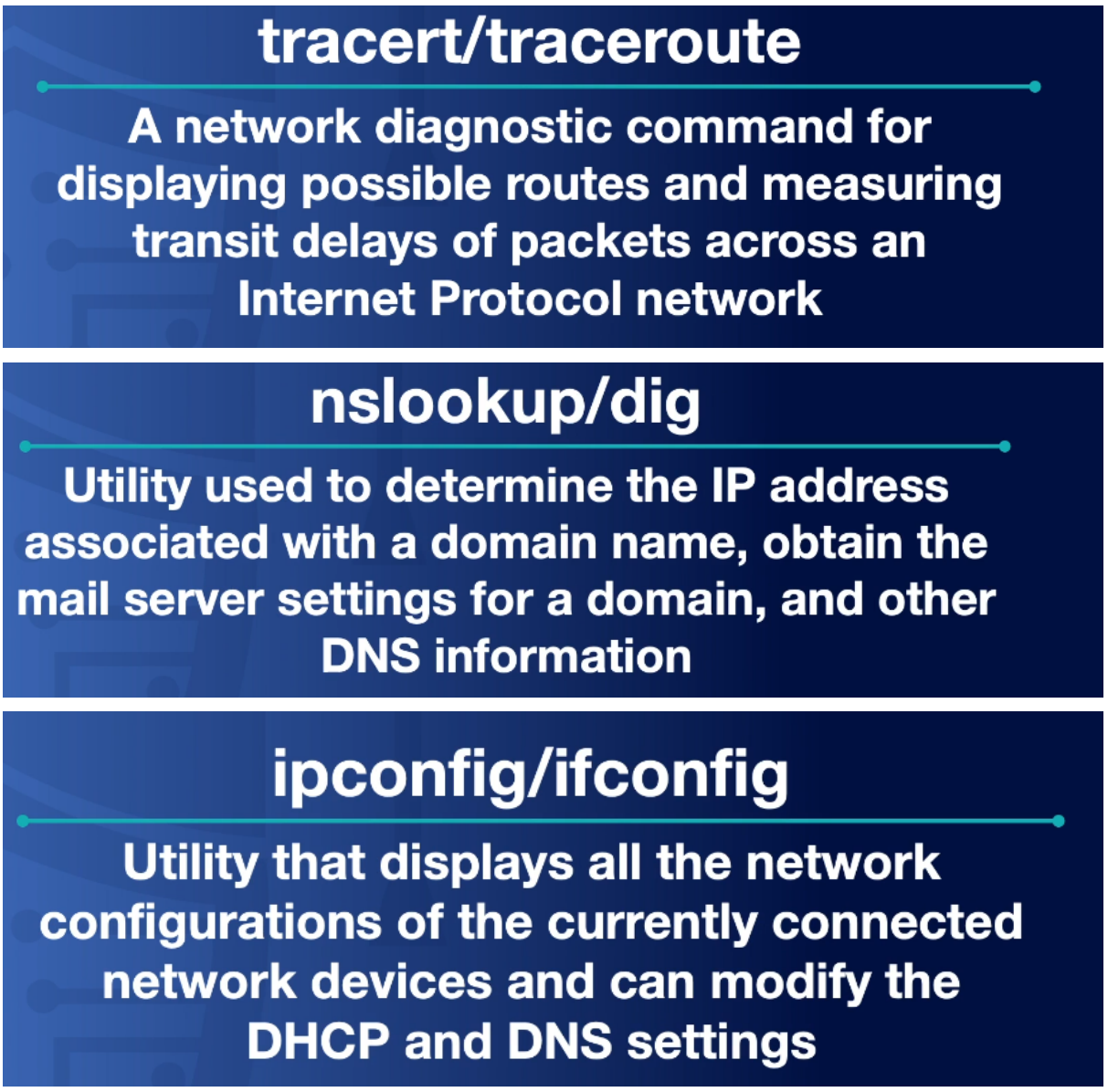
files, hidden files, and other things from the evidence drive that we collected as part of this instant response.




AccessData FTK Imager 4.1.1.1
File View Mode Help
Evidence Tree
USB2GB.dd.001
Partition 1 [1910MB]
UNTITLED [FAT32]
[root]
.fseventsd
.Spotlight-V100
.Trashes
2 - Operation TITAN CIPHER
System Volume Information
[unallocated space]
Unpartitioned Space [basic disk]
[unallocated space]
File List
Name Size Type Date Modified
.fseventsd 4 Directory 12/2/2017 2:49:...
.Spotlight-V100 4 Directory 1/21/2016 4:41:...
.Trashes 4 Directory 1/21/2016 4:41:...
2 - Operation TITAN C... 4 Directory 10/8/2016 5:28:...
System Volume Infor... 4 Directory 12/2/2017 3:00:...
!7BLAC~1.MP3 7,481 Regular File 5/31/2014 3:38:...
!7BLAC~1.MP3.FileSlack 4 File Slack
!acker.jpg 5 Regular File 12/2/2017 2:47:...
!APRIL~1.MP3 4 Regular File 4/23/2016 6:56:...
._.Trashes 4 Regular File 1/21/2016 4:41:...
._01 All I Need.mp3 4 Regular File 4/23/2016 6:56:...
._01 All I Really Want.... 4 Regular File 4/23/2016 6:56:...
._01 Anything.mp3 4 Regular File 4/23/2016 6:56:...
._01 Blitzkrieg Bop.mp3 4 Regular File 4/23/2016 6:56:...
._01 Burnout.mp3 4 Regular File 4/23/2016 6:56:...
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
Cursor pos = 0; clus = 104425; log sec = 843046; phy sec = 843048
Listed: 422 Selected: 1 USB2GB.dd.001/Partition 1 [1910MB]/UNTITLED [FAT32]/[root]/._01 Blitzkrieg Bop.mp3

Security Tools

Networking



nmap

An open-source network scanner that is used to discover hosts and services on a computer network by sending packets and analyzing their responses

ping/pathping

Utility used to determine if a host is reachable on an Internet Protocol network

hping

An open-source packet generator and analyzer for the TCP/IP protocol that is used for security auditing and testing of firewalls and networks

netstat

Utility that displays network connections for Transmission Control Protocol, routing tables, and a number of network interface and network protocol statistics

netcat

Utility for reading from and writing to network connections using TCP or UDP which is a dependable back-end that can be used directly or easily driven by other programs and scripts

arp

Utility for viewing and modifying the local Address Resolution Protocol (ARP) cache on a given host or server

route

Utility that is used to view and manipulate the IP routing table on a host or server

curl

A command line tool to transfer data to or from a server, using any of the supported protocols (HTTP, FTP, IMAP, POP3, SCP, SFTP, SMTP, TFTP, TELNET, LDAP or FILE)

the harvester

A python script that is used to gather emails, subdomains, hosts, employee names, open ports and banners from different public sources like search engines, PGP key servers and SHODAN database

sn1per

An automated scanner that can be used during a penetration test to enumerate and scan for vulnerabilities across a network

scanless

Utility that is used to create an exploitation website that can perform Open port scans in a more stealth-like manner

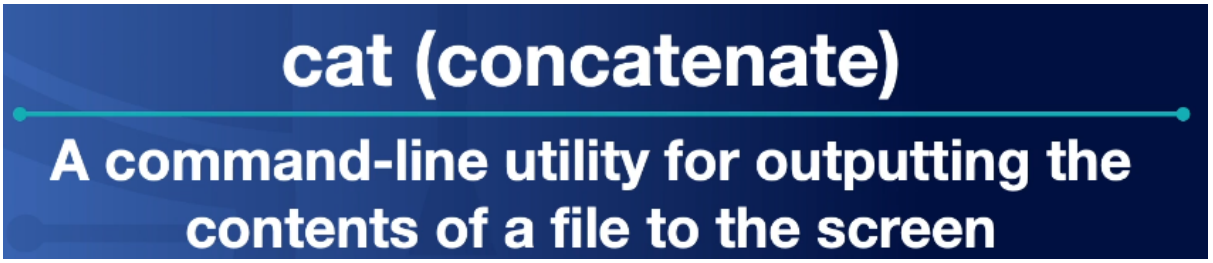
dnsenum

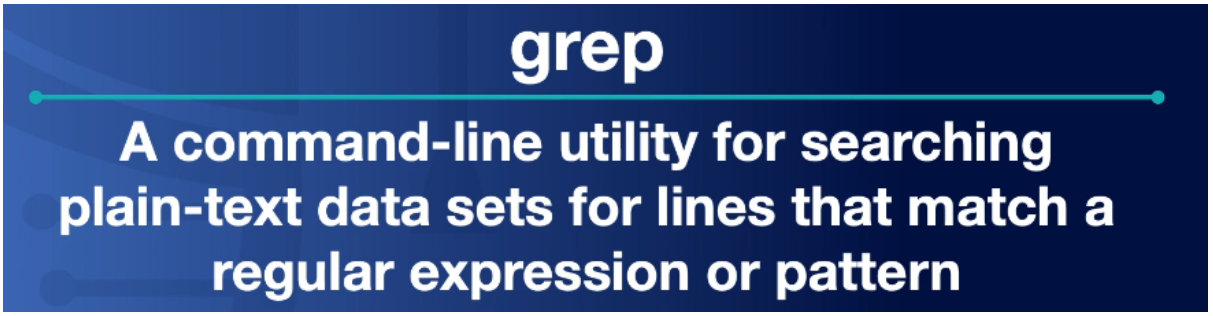
Utility that is used for DNS enumeration to locate all DNS servers and DNS entries for a given organization

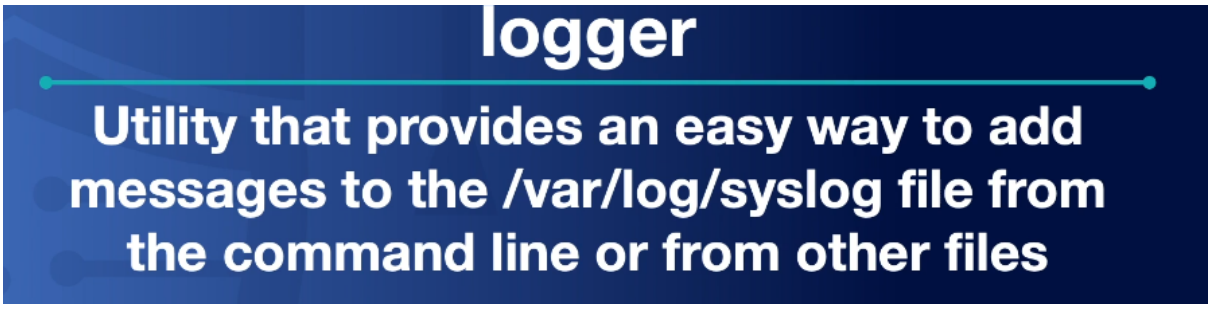
Nessus

A proprietary vulnerability scanner that can remotely scan a computer or network for vulnerabilities

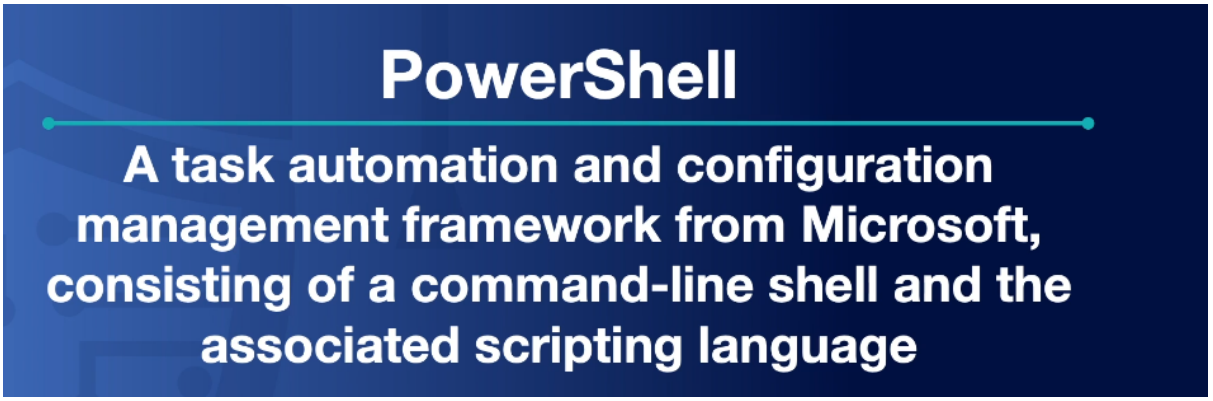
Manipulation



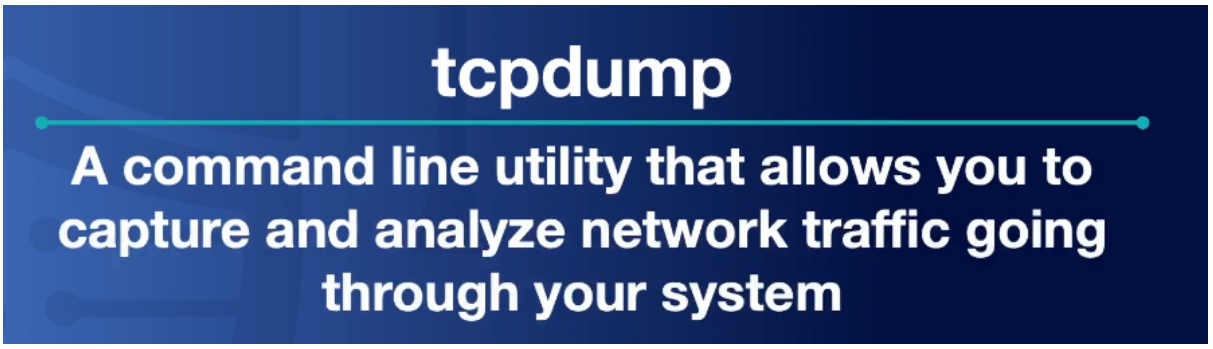




Shells and Scripts



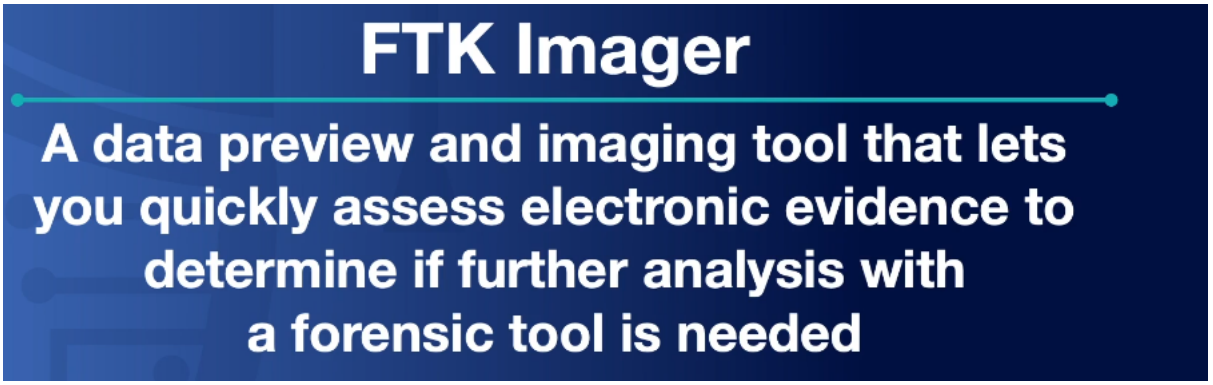
Packet Capture

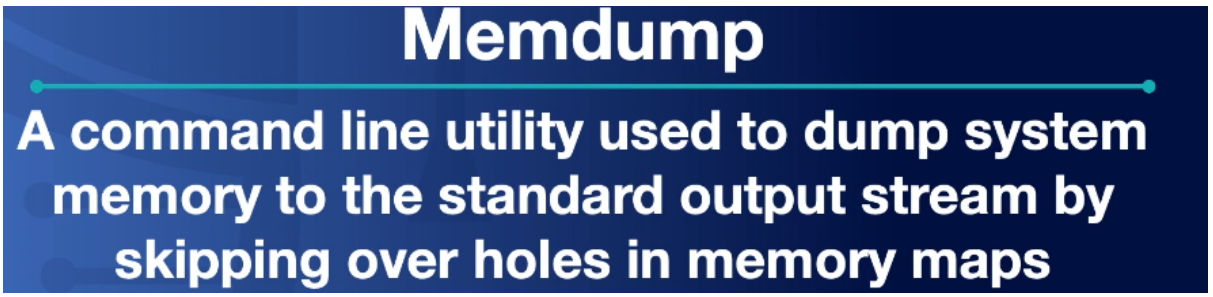



Wireshark
A popular network analysis tool to capture network packets and display them at a granular level for for real-time or offline analysis

Forensic


dd
A command line utility used to copy disk images using a bit by bit copying process


FTK Imager
A data preview and imaging tool that lets you quickly assess electronic evidence to determine if further analysis with a forensic tool is needed


Memdump
A command line utility used to dump system memory to the standard output stream by skipping over holes in memory maps

Exploitation

Browser Exploitation Framework (BeEF)

A tool that can hook one or more browsers and can use them as a beachhead of launching various direct commands and further attacks against the system from within the browser context

Cain and Abel

A password recovery tool that can be used through sniffing the network, cracking encrypted passwords using dictionary, brute-force, and cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, revealing password boxes, and analyzing routing protocols

John the Ripper

An open source password security auditing and password recovery tool available for many operating systems