MODULE -2

27. What happens when a file is deleted from windows explorer and from the command prompt? Explain

The file is not moved to the Recycle Bin at all. Instead, the file stays in the same place but its directory entry – the complete path and filename of the file – is removed and placed in a hidden folder called Recycled

The Recycle Bin is a FIFO stack: First In, First Out. That means the files you delete earliest are emptied from the Bin first. When the Recycle Bin is full, Windows starts deleting files from the Bin to make room for newly deleted files. It's only when you right-click the Recycle Bin and select Empty Recycle Bin from the pop-up menu that all files within the Bin are 'deleted'.

28.Enumerate the features of the current whole disk encryption tools. What are the hardware and software requirements of Microsoft's Bitlocker?

- Enable encryption on new IaaS VMs created from pre-encrypted VHD and encryption keys
- Enable encryption on new IaaS VMs created from the supported Azure Gallery images
- Enable encryption on existing IaaS VMs running in Azure
- Disable encryption on Windows IaaS VMs
- Disable encryption on data drives for Linux IaaS VMs
- Enable encryption of managed disk VMs
- Update encryption settings of an existing encrypted premium and non-premium storage VM
- Backup and restore of encrypted VMs

29. List some third party and open source whole disk encryption tools

VeraCrypt (Windows/OS X/Linux)

VeraCrypt is a fork of and a successor to TrueCrypt, which ceased development last year (more on them later.) The development team claims they've addressed some of the issues that were raised during TrueCrypt's initial security audit, and like the original, it's free, with versions available for Windows, OS X, and Linux. If you're looking for a file encryption tool that works like and reminds you of TrueCrypt but isn't exactly TrueCrypt, this is it. VeraCrypt supports AES (the most commonly used), TwoFish, and Serpent encryption ciphers, supports the creation of hidden, encrypted volumes within other volumes. Its code is available to review, although it's not strictly open source (because so much of its codebase came from TrueCrypt.) The tool is also under constant development, with regular security updates and an independent audit in the planning stages (according to the developers.)Those of you who nominated VeraCrypt praised it for being an on-the-fly

encryption tool, as in your files are only decrypted when they're needed and they're encrypted at rest at all other times, and most notably for being the spiritual (if not almost literal) successor to TrueCrypt. Many of you praised them for being a strong tool that's simple to use and to the point, even if it's lacking a good-looking interface or tons of bells and whistles. You also noted that VeraCrypt may not support TrueCrypt files and containers, but can convert them to its own format, which makes moving to it easy. You can read more in its nomination thread here.

AxCrypt (Windows)

AxCrypt is a free, open source, GNU GPL-licensed encryption tool for Windows that prides itself on being simple, efficient, and easy to use. It integrates nicely with the Windows shell, so you can right-click a file to encrypt it, or even configure "timed," executable encryptions, so the file is locked down for a specific period of time and will self-decrypt later, or when its intended recipient gets it. Files with AxCrypt can be decrypted on demand or kept decrypted while they're in use, and then automatically re-encrypted when they're modified or closed. It's fast, too, and allows you to select an entire folder or just a large group of files and encrypt them all with a single click. It's entirely a file encryption tool however, meaning creating encrypted volumes or drives is out of its capabilities. It supports 128-bit AES encryption only, offers protection against brute force cracking attempts, and is exceptionally lightweight (less than 1MB.) Those of you who nominated AxCrypt noted that it's really easy to use and easy to integrate into your workflow, thanks to its shell support. If you're eager for more options, it also has a ton of command line options, so you can fire up the command prompt in Windows and perform more complex actions—or multiple actions at once. It may not support the strongest or most varied encryption methods available, but if you're looking to keep your data safe from most threats, it's a simple tool that can lend a little security that your data—like files stored in the cloud on Dropbox or iCloud, for example—are secure *and* convenient to access at the same time. You can read more in this nomination thread here and here.

BitLocker (Windows)

BitLocker is a full-disk encryption tool built in to Windows Vista and Windows 7 (Ultimate and Enterprise), and into Windows 8 (Pro and Enterprise), as well as Windows Server (2008 and later). It supports AES (128 and 256-bit) encryption, and while it's primarily used for whole-disk encryption, it also supports encrypting other volumes or a virtual drive that can be opened and accessed like any other drive on your computer. It supports multiple authentication mechanisms, including traditional password and PINs, a USB "key," and the more controversial Trusted Platform Module (TPM) technology (that uses hardware to integrate keys into devices) that makes encryption and decryption transparent to the user but also comes with a host of its own issues. Either way, BitLocker's integration with Windows (specifically Windows 8 Pro) makes it accessible to many people, and a viable disk encryption tool for individuals looking to protect their data if their laptop or hard drives are lost or stolen, in case their computers are compromised, or a business looking to secure data in the field.

Of course, it goes without saying that BitLocker was a contentious nomination. More than a few of you touted BitLocker's accessibility and ease of use, and many of you even praised its encryption for being strong and difficult to crack. Many of you noted that you switched to BitLocker after the developers of TrueCrypt suggested it. Others, however, brought up the assertion made from privacy advocates that BitLocker is compromised and has backdoors in place for government security agencies (from multiple countries) to

decrypt your data. While Microsoft has officially said this isn't true and maintains there's no backdoor in BitLocker (while simultaneously maintaining the code as closed source—but available to review by its partners, which include those agencies), the assertion is enough to make more than a few of you shy away. You can read more about the criticism and controversy at the Wikipedia link above, or in the nomination thread here.

GNU Privacy Guard (Windows/OS X/Linux)

GNU Privacy Guard (GnuPG) is actually an open-source implementation of Pretty Good Privacy (PGP). While you can install the command line version on some operating systems, most people choose from the dozens of frontends and graphical interfaces for it, including the official releases that can encrypt everything from email to ordinary files to entire volumes. All GnuPG tools support multiple encryption types and ciphers, and generally are capable of encrypting individual files one at a time, disk images and volumes, or external drives and connected media. A few of you nominated specific GnuPG front-ends in various threads, like the Windows Gpg4Win, which uses Kleopatra as a certificate manager.

Those of you who nominated GnuPG praised it for being open-source and accessible through dozens of different clients and tools, all of which can offer file encryption as well as other forms of encryption, like robust email encryption for example. The key, however, is finding a front-end or a client that does what you need it to do and works well with your workflow. The screenshot above was taken using GPGTools, an all-in-one GnuPG solution that offers keychain management as well as file, email, and disk encryption for OS X. You can read more in its nomination thread here.

30. What is data acquisition? What are its types? What is its goal? Explain

Data acquisition (DAQ) is the process of measuring an electrical or physical phenomenon such as voltage, current, temperature, pressure, or sound with a computer. A DAQ system consists of sensors, DAQ measurement hardware, and a computer with programmable software. Compared to traditional measurement systems, PC-based DAQ systems exploit the processing power, productivity, display, and connectivity capabilities of industry-standard computers providing a more powerful, flexible, and cost-effective measurement solution.

31.Describe the methods for performing a remote acquisition.

- With ProDiscover Investigator you can:
  - Preview a suspect’s drive remotely while it’s in use
  - Perform a live acquisition
  - Encrypt the connection
  - Copy the suspect computer’s RAM
  - Use the optional stealth mode
- ProDiscover Incident Response additional functions
  - Capture volatile system state information
  - Analyze current running processes
  - Locate unseen files and processes
  - Remotely view and listen to IP ports

- Run hash comparisons

Create a hash inventory of all files remotely

32. What are the different tools for data acquisition? Explain

MULTI-CHANNEL PROCESS DISPLAY

Endress+Hauser

888/363-7377

Eco-Graph T multi-channel process display is a cost-effective alternative to paper recorders, data loggers and process indicators/displays. It has a USB for service and data transfer to PCs, Ethernet for integration into plant-wide systems, RS485/RS232 for integration into existing networks, an embedded web server for remote connectivity using an Internet browser, compact flash and internal memory.

VIDEOGRAPHIC BREAKOUT

ABB

215-674-6580

SM500F from ABB Instrumentation is the world's first field-mountable videographic data recorder. Its fully sealed NEMA 4X and IP66 enclosure makes it perfect for hose-down and dirty applications. Available with color or monochrome display, it can present process data in chart, bargraph and digital indicator views. Comes with a removable common SD Camera Card with a capacity of up to 2 Gbytes. Built-in Ethernet communications link to a SCADA system using Modbus TCP protocol, and is 21 CFR Part 11-compliant.

USB-BASED MULTI-FUNCTIONAL I/O

Advantech Industrial Automation Group

800/205-7940

USB-4711 is the first USB-based multifunctional I/O module. It features a 100 KS/s, 12-bit A/D converter with an on-board 1K sample FIFO buffer and provides up to 16 single-ended A/D input channels, two 12-bit D/A output channels, eight digital inputs, eight digital outputs and one event counter. Features include a USB 2.0 interface, on-board screw terminals for wiring, 16 AI, 12-bit resolution, 100KS/s, 2 AO, 8 DI and 8 DO, Windows driver, and support for ActiveX and LabView drivers.

IMPROVED SCOPE TOOL

Beckhoff Automation

952/890-0000

The redesigned Scope tool in the TwinCAT automation software suite enables users to take advantage of extended graphics featured in PCs, such as DirectX. The Logger app, which can be installed in a Windows CE control system, records the data from different channels, including PLCs and motion control packages, with time stamps and saves them intermittently. The Viewer fetches the data from the Logger by means of Beckhoff's Automation Device Specification (ADS) and displays it.

DAQ FOR MODBUS, OPC

Dataforth

520/741-1404

SCM5B isoLynx SLX200 DAQsystem implements industry-standard Modbus RTU and TCP protocols, enabling communication with a variety of existing third-party software drivers and HMI/SCADA packages. It's fully certified by Modbus-IDA and

compatible with OPC. It uses Modbus RTU for RS-232/RS-485 or Modbus TCP for Ethernet. The SLX200 combines a 6- or 12-channel I/O controller base system and optional 8- or 16-channel expansion backplanes, which can be either panel- or DIN rail-mounted. The system accepts single-channel digital or analog I/O modules. Other features include 16-bit A/D, D/A, 650+ different I/O modules, -40 °C to +85 °C operating temperature, free software configuration utility, CSA-certified, FM-approved (Class I, Division 2, Groups A, B, C, D).

33. What are the different data collection methods? Explain.

The choice of method is influenced by the data collection strategy, the type of variable, the accuracy required, the collection point and the skill of the enumerator. Links between a variable, its source and practical methods for its collection (Table 6.1, Table 6.2 and Table 6.3) can help in choosing appropriate methods. The main data collection methods are:

· Registration: registers and licences are particularly valuable for complete enumeration, but are limited to variables that change slowly, such as numbers of fishing vessels and their characteristics.

· Questionnaires: forms which are completed and returned by respondents. An inexpensive method that is useful where literacy rates are high and respondents are co-operative.

· Interviews: forms which are completed through an interview with the respondent. More expensive than questionnaires, but they are better for more complex questions, low literacy or less co-operation.

· Direct observations: making direct measurements is the most accurate method for many variables, such as catch, but is often expensive. Many methods, such as observer programmes, are limited to industrial fisheries.

· Reporting: the main alternative to making direct measurements is to require fishers and others to report their activities. Reporting requires literacy and co-operation, but can be backed up by a legal requirement and direct measurements.

34. What are the steps to create image files of digital evidence?

Step One: Capturing a Live RAM dump

This essential first step is often omitted. Yet, we strongly believe that any digital investigation must begin with acquiring a memory dump. Considering the rapidly growing popularity of whole volume encryption and cloud services, it becomes vital for an investigation to capture a volatile memory dump first, before triggering the power switch.

Memory dumps routinely contain information that could

be essential for an investigation, including binary decryption keys for encrypted volumes (TrueCrypt, BitLocker, PGP WDE), recently viewed pictures, loaded registry keys, recent Facebook communications, emails sent and received via Web services such as Gmail or Hotmail, active malware, open remote sessions, and so on.

Belkasoft offers a tiny portable tool for capturing live RAM dumps. The tool uses 32-bit and 64-bit code running in the system's most privileged kernel mode, which guarantees acquisition of the complete content of the computer's RAM even if an active anti-dumping system is running. Sized under 20KB, Belkasoft Live RAM Capturer ensures minimum acquisition footprint while preserving the maximum amount of data.

The forensically sound tool is portable, read-only and ready to run out of the box.

Please note that we don't use a proprietary format to store memory dumps. The resulting memory image can be processed by Belkasoft Evidence Center as well as many other commercial tools with similar functionality.

Step Two: Acquiring a Disk Image

Creating a forensic image of the suspect's hard drive is an essential step and a must-do in any investigation. We offer a combination of hardware and software to help acquire forensic disk images while overcoming all possible issues.

- The hardware is designed to acquire hard drives damaged to the point where competing

imaging products stall.

- You are in full control of how to process reading errors. The product notifies you of any issues immediately, without the need to wait till the imaging completes.
- You can bypass ATA passwords including those found in the latest SATA 6 drives.
- You can reset HPA/DCO if present.

The hardware supports cloning and imaging to a file, enabling you to make up to 3 copies of the source device with a SATA, IDE and USB interface. The receiving device can be a SATA, SSD or USB drive or a file on your computer. You can upload the image onto a remote PC via an Ethernet connection. Full remote operation is supported allowing you to control the imaging process from another location.

Please note that we don't use a proprietary format to store drive images. The resulting images can be processed by Belkasoft Evidence Center as well as many other commercial tools with similar functionality.

Step Three: Discovering and Analyzing Evidence

During this step, you may have multiple images created with Belkasoft Live RAM Capturer as well as the disk imaging tool. The supplied analytic tool, Belkasoft Evidence Center, will help you get the most out of these images, retrieving existing and deleted

evidence in full auto mode. With hundreds of formats supported, the tool will quickly extract you the most forensically important information.

The following types of data can be located or recovered if deleted:

- Office documents
- Emails
- Pictures
- Videos
- Mobile application data
- Web browser histories, cookies, passwords, cache, etc.
- Chats and instant messenger histories
- Social network communications
- System files including jumplists, thumbnails and event logs
- Encrypted files
- Registry files
- SQLite databases
- PCAP files

Belkasoft Evidence Center accepts memory images and disk images in all popular forensic formats, allowing you to process images acquired with non-Belkasoft imaging tools. The following data sources are supported:

- EnCase E01 and Ex01 images
- FTK images
- UFED physical dumps for mobile phones
- DD images
- SMART images
- Mobile chip-off dumps
- VMWare and Virtual PC files
- Hibernation and page files

Belkasoft Evidence Center processes the following systems:

- Windows
- Mac OS X
- Linux/Unix
- iOS
- Android
- Blackberry

The following types of analysis are available:

- Search and analysis of existing and deleted files
- Data carving and destroyed evidence recovery
- Live RAM analysis
- Hibernation and page file analysis
- Native SQLite analysis with freelist support (discovers deleted SQLite records, e.g. Skype conversations, WhatsApp messages, iPhone deleted SMS/text messages, Chrome downloads etc.)
- Picture/photo analysis including EXIF and GPS analysis, face/pornography/text/forgery detection
- Video key frame extraction
- Encryption detection
- Network traffic analysis
- And many others

You can also purchase Belkasoft Evidence Center standalone. We offer a free trial of this product; to request the free evaluation version, please refer to http://belkasoft.com/trial.

Step Four: Creating Reports, Sharing Evidence, Getting Ready for a New Case

Belkasoft Evidence Center allows you to create reports in all most popular formats: from PDF and HTML to XLSX and XML. The report options are highly customizable, resulting report can be presented in court or shared with a colleague.

Portable Belkasoft Evidence Reader tool, which is included into the Suite, allows users to share evidence, collected with the help of Evidence Center. Even users without license of Acquisition & Analysis Suite can review collected data using Evidence Reader.

35. Making a bit-stream image is simple in theory, but the accuracy of the backup must meet evidence standards.

i. How do we verify the accuracy of a bit stream copy?

The growth in the computer forensic field has created a demand for new software (or increased functionality to existing software) and a means to verify that this software is truly forensic (i.e., capable of meeting the requirements of the trier of fact). In this work, we present a function-oriented testing framework for validation and verification of

computer forensic tools. This framework consists of three parts: function mapping, requirements specification, and reference set development. Through function mapping, we give a scientific and systemical description of the fundamentals of computer forensic discipline; i.e., what functions are needed in the computer forensic investigation process. We focus this article on the forensic copy function. We specify the requirements and develop and a corresponding reference set to test any tools that possess the forensic copy function.

ii. Name and explain a hashing technique used for verification.

Snefru

- a one-way hash function designed by Ralph Merkle
- creates 128 or 256 bit long hash values (let m be length)
- uses an algorithm H which hashes 512-bits to m-bits, taking the first m output bits of H as the hash value
    - H is based on a reversible block cipher E operating on 512-bit blocks
    - H is the last m-bits of the output of E XOR'd with the first m-bits of the input of E
    - E is composed of several passes, each pass has 64 rounds of an S-box lookup and XOR
    - E can use 2 to 8 passes
- overview of algorithm
    - break message into 512-m bit chunks
    - each chunk has the previous hash value appended (assuming an IV of 0)
    - H is computed on this value, giving a new hash value
    - after the last block (0 padded to size as needed) the hash value is appended to a message length value and H computed on this, the resulting value being the MAC
- Snefru has been broken by a birthday attack by Biham and Shamir for 128-bit hashes, and possibly for 256-bit when 2 to 4 passes are used in E
- Merkle recommends 8 passes, but this is slow

MD2, MD4 and MD5

- family of one-way hash functions by Ronald Rivest
- MD2 is the oldest, produces a 128-bit hash value, and is regarded as slower and less secure than MD4 and MD5
- MD4 produces a 128-bit hash of the message, using bit operations on 32-bit operands for fast implementation

R L Rivest, "The MD4 Message Digest Algorithm", Advances in Cryptology - Crypto'90, Lecture Notes in Computer Science No 537, Springer-Verlag 1991, pp303-311

- MD4 overview

- pad message so its length is 448 mod 512
- append a 64-bit message length value to message
- initialise the 4-word (128-bit) buffer (A,B,C,D)
- process the message in 16-word (512-bit) chunks, using 3 rounds of 16 bit operations each on the chunk & buffer
- output hash value is the final buffer value

- some progress at cryptanalysing MD4 has been made, with a small number of collisions having been found
- MD5 was designed as a strengthened version, using four rounds, a little more complex than in MD4 [2]
- a little progress at cryptanalysing MD5 has been made with a small number of collisions having been found
- both MD4 and MD5 are still in use and considered secure in most practical applications
- both are specified as Internet standards (MD4 in RFC1320, MD5 in RFC1321)

36. What is a bit-stream image? How is it created? Explain

A bit-stream image is a sector-by-sector / bit-by-bit copy of a hard drive. A bit-stream image is actually a set of files that can be used to create an exact copy of a hard drive, preserving all latent data in addition to the files and directory structures. A bit-stream image can be read by the majority of the tools used by the Computer Forensics Examiner to analyze the hard drive such as Encase, FTK, ProDiscover and many others. By utilizing the bit-stream image, the Computer Forensics Examiner takes no risk of contaminating the original evidence.

The Computer Forensics Examiner creates the bit-stream image by attaching the original computer media to a write protection device that ensures no writes can take place to the original media while the bit-stream image is created.

37. Give a sample evidence custody form. What are its functions?

I. INTRODUCTION.

We can only cover both the federal and California law of evidence in a brief essay like this by a ruthless process of selection and compression. What we will cover can best be thought of as that essential kernel of the law of evidence that the trial lawyer must carry in his head.

Our task would be impossible but for two important facts. First, all of you have studied the law of evidence before, either in a course on evidence or in preparation for the bar exam. Accordingly, most of the rules presented will already be familiar to you. What we will do here is to try to review, organize, and reinforce that law so that you can apply it with confidence when you need it.

Second, most of the rules of evidence need not be covered here because they are either so obvious that you already know all you need to know about them or they apply only in limited circumstances. For example, we would surely be wasting our time if we indulged in an extended discussion of the rule that evidence should be construed to achieve the ends of justice, and others like it. This and many other rules only state the obvious and will not be covered here. Rules that apply only in limited circumstances include ones like those relating to the scope of cross examination of a plaintiff in a case of sexual assault, a juror's incompetence to impeach his own verdict, and the proof of valuation of property. Evid. Code §§ 781, 1150, 810 et seq.; Fed. Rules Evid. 412, 606. You do not need to know those special rules unless you get a case where they apply. When that happens, it will be time enough to study them.

What is left after you eliminate all the rules that are obvious and all those that have only limited application are the rules that are used every day in ordinary cases and that are not trivial or obvious. These essential tools of survival must be thoroughly mastered. They will enable you to solve the vast majority of evidentiary problems that arise in preparing and trying your cases.

I do recommend, however, that you take the time to read whichever codification applies to your practice so you will know when you need to study one of the rules of limited application and so that you can gain confidence that there are not any gaps in your knowledge.

California's Evidence Code is short and the Federal Rules of Evidence are shorter and, once we are done, I think that you will have an analytic framework that will allow you to read them easily and with understanding.

II. THE FOUR TYPES OF EVIDENCE.

There are four traditional types of evidence: real, demonstrative, documentary, and testimonial. Some rules of evidence apply to all four types and some apply only to some or one of them. First, we will cover general rules of admissibility that apply to all evidence. Then, we will cover foundational rules that relate to specific kinds of evidence. Finally, we will cover some special topics, like the form of examination, the hearsay rule, and the lay opinion rule, that frequently cause problems in the courtroom.

III. GENERAL RULES OF ADMISSIBILITY.

The basic prerequisites of admissibility are relevance, materiality, and competence. In general, if evidence is shown to be relevant, material, and competent, and is not barred by an exclusionary rule, it is admissible. Evid. Code § 351; Fed. Rules Evid. 402.

Evidence is relevant when it has any tendency in reason to make the fact that it is offered to prove or disprove either more or less probable. Evid. Code § 210; Fed. Rules Evid. 401. To be relevant, a particular item of evidence need not make the fact for which it is offered certain, or even more probable than not. All that is required is that it have some tendency to increase the likelihood of the fact for which it is offered. Weighing the evidence is for the finder of fact, and although a particular piece of evidence, standing by itself, may be weak, it will be admitted unless it is otherwise incompetent or it runs afoul of an exclusionary rule. For example, if the fact to be proved is that the defendant bit off the plaintiff's nose in a fight, testimony by an eyewitness to the act would clearly be relevant, but so would testimony by a witness who heard the plaintiff and the defendant exchange

angry words on the day before the fight, or even testimony by a witness who sold the defendant a disinfectant mouthwash shortly afterwards.

Evidence is material if it is offered to prove a fact that is at issue in the case. For example, if I offer the testimony of an eyewitness to prove that it was raining on the day of the signing of a contract, that evidence may be relevant to prove the fact for which it is offered, yet the fact that it was or was not raining may be immaterial to any of the issues in the case, which may turn entirely on whether one or both parties breached the contract.

The issues in the case are determined by the pleadings, any formal stipulations or admissions, and the applicable law. For example, if, in a case of breach of contract, the defendant has conceded that the plaintiff performed all his covenants, proof of that performance would no longer be material unless it were relevant to some other issue. Under both the California and federal rules, the concept of materiality is included in the concept of relevance. Evid. Code § 210; Fed. Rules Evid. 410.

Evidence is competent if the proof that is being offered meets certain traditional requirements of reliability. The preliminary showing that the evidence meets those tests, and any other prerequisites of admissibility, is called the foundational evidence. Evid. Code § 402, 403. When an objection is made that an answer to a question, a document, or a thing lacks a proper foundation, what the objector is really saying is that a showing of competence, or of another prerequisite of admissibility, has not yet been made. The modern trend in the law is to diminish the importance of the rules of competence by turning them into considerations of weight. *See*, e.g., Evid. Code § 700; Fed. Rules Evid. 601. The question of competence will be considered below for each category of evidence.

In general, if competent evidence is offered to prove a relevant and material fact, it is admissible even if it would have been improper to receive it for another purpose. Evid. Code § 355. For example, while evidence of prior bad acts is generally not admissible to show that a person acted similarly in the present case, it may be admissible to show motive, plan, intent, lack of mistake or, in federal court, to impeach a witness's credibility. Evid. Code § 1101(b); Fed. Rules Evid. 404(b). When evidence is received for a limited purpose, the party who thinks a jury may make improper use of that evidence is entitled, upon his request, to a limiting instruction. Evid. Code § 355.

However, where the value of evidence for its proper purpose is slight and the likelihood that it will be used for an improper purpose by a finder of fact is great, a court may, in its discretion, exclude the evidence even though it would otherwise be admissible. Evid. Code § 352; Fed. Rules Evid. 403. In this situation, the probative value of the evidence is said to be outweighed by its prejudicial effect.

Prejudice means improper harm. The fact that evidence may be extremely harmful to one party's case does not necessarily make it prejudicial. Courts also have discretion to exclude otherwise admissible evidence to prevent confusion, delay, waste of time, or the needless presentation of cumulative evidence. Evid. Code § 352; Fed. Rules Evid. 403.

IV. REAL EVIDENCE.

Real evidence is a thing the existence or characteristics of which are relevant and material. It is usually a thing that was directly involved in some event in the case. The written contract upon which an action is based is real evidence both to prove its terms and that it was executed by the defendant. If it is written in a faltering and unsteady hand, it may also

be relevant to show that the writer was under duress at the time of its execution. The bloody bloomers, the murder weapon, a crumpled automobile, the scene of an accident--all may be real evidence.

To be admissible, real evidence, like all evidence, must be relevant, material, and competent. Establishing these basic prerequisites, and any other special ones that may apply, is called laying a foundation. The relevance and materiality of real evidence are usually obvious. Its competence is established by showing that it really is what it is supposed to be. Proving that real or other evidence is what it purports to be is called authentication. Evid. Code § 1400; Fed. Rules Evid. 901.

Real evidence may be authenticated in three ways--by identification of a unique object, by identification of an object that has been made unique, and by establishing a chain of custody. You only have to be able to use one of these ways, though it is prudent to prepare to use an alternate method in case the court is not satisfied with the one you have chosen.

- The easiest and usually the least troublesome way to authenticate real evidence is by the testimony of a witness who can identify a unique object in court. For example, the curator of a museum may be able to testify that he is familiar with, say, Picasso's "Dames de Avignon" and that what has been marked as exhibit so-and-so is in fact that unfortunate painting. It is important to remember, however, that many more mundane objects may be amenable to this kind of identification. A unique contract, or one that has been signed, may be authenticated by a person who is familiar with the document or its signatures. A ring may have an inscription by which it can be identified. Even a manufactured object, like a wallet, may be identifiable by its owner after years of use have given it a unique personality.
- The second method--identification in court of an object that has been made unique, is extremely useful since it sometimes allows a lawyer or client to avoid the pitfalls of proving a chain of custody by exercising some forethought. If a witness who can establish an object's relevance to the case marks it with his signature, initials, or another mark that will allow him to testify that he can tell it from all other objects of its kind, that witness will be allowed to identify the object in court and thus to authenticate it. Often, if a member of the lawyer's staff or another person early in the chain of custody marks the evidence, big problems can be avoided if a later link in the chain turns out to be missing.
- The third and least desirable way to authenticate real evidence is by establishing a chain of custody. Establishing a chain of custody requires that the whereabouts of the evidence at all times since the evidence was involved in the events at issue be established by competent testimony.

The proponent of the evidence must also establish that the object, in relevant respects, has not changed or been altered between the events and the trial. This can sometimes be a tall order, or can require the testimony of several witnesses. If there is any time from the events in question to the day of trial during which the location of the item cannot be accounted for, the chain is broken. In that case, the evidence will be excluded unless another method of authentication can be used.

V. DEMONSTRATIVE EVIDENCE.

Demonstrative evidence is just what the name implies--it demonstrates or illustrates the

testimony of a witness. It will be admissible when, with accuracy sufficient for the task at hand, it fairly and accurately reflects that testimony and is otherwise unobjectionable. Typical examples of demonstrative evidence are maps, diagrams of the scene of an occurrence, animations, and the like. Because its purpose is to illustrate testimony, demonstrative evidence is authenticated by the witness whose testimony is being illustrated. That witness will usually identify salient features of the exhibit and testify that it fairly and accurately reflects what he saw or heard on a particular occasion, such as the location of people or things on a diagram.

For some time in California, and in some other states, there was a controversy over whether photographs were only demonstrative in nature or whether they had evidentiary value independent of the testimony of the witness who authenticated them. This problem was particularly pressing when there was no witness who could confirm what the camera saw as, for example, where crucial identifying photographs were taken by automatic cameras.

Fortunately, the courts in California and most other states seem to have reached the only sensible solution, which is that photographs can be either real or demonstrative evidence depending on how they are authenticated. When a photograph is authenticated by a witness who observed what is depicted in it and can testify that it accurately reflects what he saw, the photograph is demonstrative evidence. When it is authenticated by a technician or other witness who testifies about the operation of the equipment used to take it, it is real evidence and is, in the language of the courts, a "silent witness."

VI. DOCUMENTARY EVIDENCE.

Documentary evidence is often a kind of real evidence, as for example where a contract is offered to prove its terms. When a document is used this way it is authenticated the same way as any other real evidence--by a witness who identifies it or, less commonly, by witnesses who establish a chain of custody for it. However, because they contain human language, and because of the historical development of the common law, documents present special problems not presented by other forms of real evidence, such as when they contain hearsay.

When dealing with documentary evidence, it is a good idea to ask yourself four questions:

1. Is there a parol evidence problem?
2. Is there a best evidence problem?
3. Is there an authentication problem?
4. Is there a hearsay problem?

The parol evidence rule, which bars the admission of extrinsic evidence to vary the terms of a written agreement, is usually considered a matter of substantive law, not of rule of evidence. Accordingly, we will not deal with it here.

As has been noted above, documents can be authenticated the same way as any other real evidence. Evid. Code § 1400, 1401, 1410-1416. Material alterations must be accounted for. Evid. Code § 1402. There are also specifically approved methods of authenticating documents listed in the Evidence Code, including the submission to the finder of fact of a known exemplar of a signature for comparison with the signature on a disputed document, Evid. Code § 1417, authentication by evidence of a reply, Evid. Code § 1420, and

authentication by content, Evid. Code § 1421.

In addition, some documents, such as certified copies of public records, official documents, newspapers, periodicals, trade inscriptions, acknowledged documents to prove the acknowledgment, certificates of the custodians of business records, and certain commercial paper and related documents are, to one extent or another, self authenticating under either California law or the federal rules. Evid. Code § 1450 et seq., 1530 et seq., 1562; Fed. Rules Evid. 901, 902.

We will cover the hearsay rule as a separate topic.

The best evidence rule provides that, where a writing is offered in evidence, a copy or other secondary evidence of its content will not be received in place of the original document unless an adequate explanation is offered for the absence of the original. Evid. Code § 1500 et seq.; Fed. Rules Evid. 1002. In California, testimonial and other secondary evidence of the document's content is also generally forbidden. Evid. Code §§ 1500, 1508.

The best evidence rule arose during the days when a copy was usually made by a clerk or, worse, a party to the lawsuit. Courts generally assumed that, if the original was not produced, there was a good chance of either a scrivener's error or fraud. Now that "copy" usually means "photocopy," the chance of a copy being in error, as opposed to simply illegible, is slight. In addition, courts are reluctant to require needless effort and delay where there is no dispute about the fairness and adequacy of a photocopy.

Accordingly, both California law and the federal rules allow the use of mechanically produced duplicates unless a party has raised a genuine question about the accuracy of the copy or can show that its use would be unfair. Evid. Code §§ 1500 et seq.; Fed. Rules Evid. 1003. However, there is always a danger of a party questioning a document, so it is important to remember that, unless you have a stipulation to the contrary, or your document fits one of the exceptions listed in the statute, you must be ready to produce originals of any documents involved in your case or to produce evidence of why you can't.

Under both California law and the federal rules, compilations or summaries of voluminous records may be received where the originals are available for examination by the other parties. Evid. Code § 1509.

VII. TESTIMONIAL EVIDENCE.

Testimonial evidence is the most basic form of evidence and the only kind that does not usually require another form of evidence as a prerequisite for its admissibility. See Evid. Code § 702(b); Fed R. Evid. 602. It consists of what is said in the court at the proceeding in question by a competent witness.

In general, a witness is competent if he meets four requirements:

1. He must, with understanding, take the oath or a substitute. Evid. Code §§ 710, 701; Fed. Rules Evid. 603.
2. He must have personal knowledge about the subject of his testimony. In other words, the witness must have perceived something with his senses that is relevant to the case. Evid. Code § 702; Fed. Rules Evid. 602.
3. He must remember what he perceived.
4. He must be able to communicate what he perceived. Evid. Code § 701(a)(1).

There are other rules of competence that relate to special circumstances, such as the rule that a juror is generally incompetent to impeach his own verdict or that, at least in federal court, a judge is not competent to testify in a trial over which he is presiding, but these and other rules like them rarely come up in practice. Evid. Code §§ 1150, 703; Fed. Rules Evid. 606, 605.

In addition, in keeping with the modern trend to view issues that were previously thought to involve questions of competence, which could result in the exclusion of evidence, as presenting instead questions of weight for the finder of fact to evaluate, the rules of competence are very liberally construed and will rarely result in the exclusion of evidence. For example, the requirement that a witness take the oath or a substitute permits virtually any kind of affirmation by which the witness, in effect, promises to tell the truth. Evid. Code § 165. The "understanding" of the oath or affirmation that is required can be that of a small child or mentally disabled person. Evid. Code § 701, 710; *People v. McIntyre* (1967) 256 Cal.App.2d 894, 898; 64 Cal. Rptr. 530, 533. The communication that is required may be in writing or through an interpreter, whether of spoken or of sign language. Evid. Code § 701, 752, 754; Fed. Rules Evid. 604. In addition, deficiencies in knowledge generally affect only weight, so long as the witness perceived something relevant.

Even if a witness forgets what he is supposed to be testifying about, the law allows you to supplement his memory.

- First, you can ask for a recess so that the witness can walk around and calm his nerves.
- Second, you can ask a leading question to try to refresh his recollection. This is an exception to the usual rule against the use of leading questions during direct examination.
- Third, you can attempt to refresh the witness's recollection in another way.

This method is commonly called "past recollection refreshed." Before you can try to refresh the witness's memory he must say that he can't remember the fact you are trying to elicit. Then he must say that the refreshing object might help him remember. Anything that the witness says might help him may be used--his own notes, notes or documents prepared by others, a videotape of events, the smell of a decedent's perfume, a snow-cone, or a recording of the Beach Boys singing "Surf City USA." If the memory refresher is a writing, it must be provided to opposing counsel. This is true whether the witness looks at it on the stand or before he testifies, as for example, during preparation by counsel. In California, the unexcused failure to produce writings that have been used by a witness to refresh his memory will result in his testimony being stricken! Evid. Code § 771. The witness is permitted to look at, smell, listen to, touch, or taste the memory refresher. When he is done, you withdraw it from him and ask whether he can now remember the fact you are interested in. If, after all this, the witness remembers what you are after, he is permitted to answer. Fed. Rules Evid. 612.

The memory refreshing thing is not evidence and cannot be received as such, though it must be made available to the opposing party and may be used by him for cross examination or for any other proper purpose, including the introduction of portions of it that relate to the witness's testimony. Fed. Rules Evid. 612. With present recollection refreshed, it is the answer of the witness, after his memory has been refreshed, that is

evidence. Of course, your adversary may comment on the frailty of your witness's memory when he argues about the weight to be attached to the testimony.

Even if your efforts to fan the embers of memory with memory refreshers fail to produce a flame, there is still hope. If the witness has previously recorded, directed the recording of, or verified the accuracy of a writing or other portrayal of the fact you are interested in, you can use the fourth method of aiding or supplementing his memory by offering the writing as a past recollection recorded. Evid. Code § 1237. First, the witness must say that he no longer remembers the fact. Then you try to refresh the witness's memory with the writing or other recording you intend to use. If you can refresh the witness's memory, he will be permitted to answer the question. If the writing fails to refresh the witness's memory, he must identify it as one that he made or saw when he did remember the fact in question and that he knew then that the writing was accurate. Evid. Code § 1237. With past recollection recorded, the witness never answers the question and the writing is the evidence.

Because it is an out of court statement that is offered to prove the truth of its content, a past recollection recorded is hearsay. However, it is admissible under its own exception to the hearsay rule. Evid. Code § 1237(a); Fed. Rules Evid. 803(5). In addition, like any other documentary evidence, a past recollection recorded must meet the requirements of the best evidence rule. Unlike other documentary evidence, while a past recollection recorded may be read into the record, it may not be shown to the jurors or taken with them when they retire to deliberate. *Id*.

Bias, interest, prejudice, and other grounds to doubt the credibility of a witness go only to the weight of his testimony and do not affect his competence. In particular, it is not a valid objection to say that a statement by a witness is "self-serving." Presumably, most or all statements by party witnesses are or are intended to be self serving.

VIII. FORM OF EXAMINATION.

On direct examination, you are generally not permitted to ask leading questions. Fed. Rules Evid. 611(c). Direct examination is questioning by the lawyer who calls the witness to testify concerning matters that into which he is the first party to inquire. Evid. Code § 760. A leading question is one that suggests an answer or substitutes the words of the lawyer for those of the witness. These are questions like "You told the defendant that you were relying on him for advice, didn't you?"

Questions that call for an answer of "yes" or "no" are not necessarily leading. For example, most courts would allow you to ask a question like "Did you ever tell the defendant that you wanted the goods?" However, questions that call for a yes or no answer can be leading if they form a pattern that leads the witness through his testimony or reduces the witness to adopting the descriptions of his lawyer. For example, the following is clearly leading:

Q: When you entered the room did you see the defendant there?
A: Yes.
Q: Was he visibly agitated?
A: Yes.
Q: Did you ask him whether he intended to deliver the goods you had ordered?
A: Yes.
Q: Did he tell you that he had no intention of doing so?
A: Yes.

Other cases are not so clear:

Q: When you met the defendant that night, what was his physical condition?
A: He was swaying from side to side.
Q: Did he seem to you to be drunk?
A: Yes.

As you can see, in many ways, leading is a matter of degree, and borderline cases are matters of judgment and within the court's discretion, as is the question of when to allow such leading questions on direct. Most of the time, when an objection is sustained to a leading question, it is not difficult to rephrase the question to make it unobjectionable:

Q: When you saw the defendant that night, was he drunk?
Counsel: Objection. Leading.
Court: Sustained.
Q: What was the defendant's physical condition when you saw him?
A: He was drunk as a skunk.

As this last exchange shows, not only is eliciting testimony with nonleading questions proper, it is also usually more effective to let the witness tell the story if he can.

Leading questions are permitted on direct in several circumstances. We have already discussed the propriety of a leading question to refresh a witness's recollection. Leading questions are also usually permitted in dealing with matters of background, or to direct the witness's attention to a particular time and place or to a particular aspect of a situation. For example, the following should usually be permitted:

Q: Were you at Sloppy Louie's on the evening of the twenty fifth of January?
A: Yes.
Q: Did you see the defendant's car parked outside?
A: Yes.
Q: Was there anyone inside the car?
A: Yes.
Q: Who?
A: The defendant, that dirty rotten skunk.
Counsel: I move to strike everything after "the defendant" as unresponsive, irrelevant, incompetent, immaterial, and prejudicial.
Court: So stricken.

In the example above, while part of the witness's answer was objectionable for other reasons, the questioning would probably not be considered improper, although the first three questions might be considered leading.

Leading questions may be allowed where, in the judge's sound discretion, they will help to elicit the testimony of a witness who, due to tender age, incapacity, or limited intelligence, is having trouble communicating his evidence. Fed. Rules Evid. 611(c). They are also allowed when examining an adverse or hostile witness. Evid. Code § 776; Fed. Rules Evid. 611(c). Witnesses are adverse or hostile when their interests or sympathies are likely to lead them to resist testifying forthrightly or who fall into certain defined categories. Generally, an adverse party or a witness identified with an adverse party is considered hostile for the purposes of this rule. Evid. Code § 776; Fed. Rules Evid. 611(c).

The converse of a leading question is one that calls for a narrative answer. Questions that require a witness to tell a story without responding to specific questions deprive your opponent of the opportunity to interpose an objection before the witness says something that is inadmissible. They often also elicit rambles that waste the time of the court and the parties. The following is an example:

Q: What happened next?
A: Then Smittie told me about how he had seen the defendant attack the plaintiff from behind with a baseball bat.
Counsel: I move to strike that entire answer as hearsay.
Court: So stricken. The jury is instructed to disregard the last answer.

Of course, the damage may already be done.

The problem with the "leading" rule and "narrative" rule is that, if they are both interpreted broadly, they can completely prevent any meaningful examination. This is an area where the advocate must be alert to the judge's preferences.

On cross examination, leading questions are generally permitted and often necessary or desirable. Evid. Code § 767; Fed. Rules Evid. 611(c). Harassment of the witness is not. Evid. Code § 765; Fed. Rules Evid. 611(a).

Cross examination is only permitted to inquire into subjects that were raised upon direct, including credibility. Evid. Code § 761; Fed. Rules Evid. 611(b). If the cross examiner strays into a new area, the judge has the discretion to permit him to do so, in effect permitting him to present part of his case out of turn for the sake of efficiency or other good cause. Evid. Code § 320, 772; Fed. Rules Evid. 611(b). However, for the purposes of eliciting the new matter, the witness is considered to have been adopted by the cross examiner and counsel is therefore required to confine himself to the kind of questioning permitted for direct examination. *Id*. If, on redirect, the original sponsor of the witness explores the new subjects, he is permitted the same latitude that is allowed in a normal cross examination.

IX. THE LAY OPINION RULE.

Witnesses are required to give their answers in the form of statements of what they saw, heard, felt, tasted, or smelled. They are generally forbidden to express opinions or draw conclusions. As anyone who gives the matter any thought soon discovers, this distinction between fact and opinion is not always clear. In addition, many witnesses find it impossible to give their testimony in the required form, and certain perceptions are very difficult to communicate without using language that suggests judgments and opinions. *Osborn v. Mission Ready Mix* (1990) 224 Cal. App.3rd 104, 112-113; 273 Cal Rptr. 457, 461-462. As a result, both California law and the federal rules have substantially relaxed the rule against lay opinions to facilitate the reception of evidence.

In general, a person who is not testifying as an expert will be allowed to testify in the form of an opinion if the opinion is both rationally based on his perception and helpful to an understanding of his testimony. Evid. Code § 800; Fed. Rules Evid. 701. In addition to this general rule, opinions by a competent layperson on certain subjects are specifically permitted by rule, statute, or cases. Some of these are:

1. A person's identity, whether identified by appearance, voice, or otherwise. *Corey v.*

Corey (1964) 230 Cal.App.2d 813, 826, 41 Cal.Rptr. 379, 387; Fed. Rules Evid. 901(b)(4)-(6).

2. A person's sanity. Evid. Code § 870.
3. Quantities, such as speed, distance, and size. *Rash v. City and County of San Francisco* (1962) 200 Cal. App.2d 199, 204, 19 Cal.Rptr. 266, 269.
4. Demeanor, mood, or intent. *People v. Deacon* (1953) 117 Cal.App.2d 206, 210, 255 P.2d 98; *People v. Harris* (1969) 270 Cal.App.2d 863, 872, 76 Cal.Rptr. 130, 137 (testimony that a person was "trying" to break up a fight).
5. Intoxication or sobriety. *In re Joesph G.* (1970) 7 Cal App.3d 695, 704, 764, 87 Cal.Rptr. 25, 31.
6. Physical condition of health, sickness, or injury. *Waite v. Goodfrey* (1980) 106 Cal.App.3d 760, 764, 163 Cal.Rptr. 881, 883.
7. Ownership. *Strauss v. Dubuque Fire & Marine Ins. Co.* (1933) 132 Cal.App. 283, 294, 22 P.2d 582.
8. The value of one's own property. Evid. Code § 813; *Schroeder v. Auto Driveaway Co.* (1974) 11 Cal.3d 908, 921, 114 Cal.Rptr. 622, 630.
9. Identification of handwriting. Evid. Code § 1416; Fed. Rules Evid. 901(b)(2).

Opinion testimony is not objectionable merely because it embraces the ultimate issue to be decided. Evid. Code § 805; Fed. Rules Evid. 704(a). This is true notwithstanding a common misunderstanding to the contrary among some old timers.

X. ACCREDITING AND DISCREDITING A WITNESS.

A witness may not be accredited until he has first been impeached. Under both California law and the federal rules, any party may impeach any witness at any time. Evid. Code § 785; Fed. Rules Evid. 607.

A witness's credibility could traditionally be impeached by inquiry into any of nine areas. The first four of these nine areas relate to the requirements of competence. They are:

1. The firmness and sincerity of the witness's belief that any violation of his oath could have eternal consequences. This method is probably no longer available. See Fed. Rules Evid. 610.
2. The quality of witness's perception or ability to perceive. Evid. Code § 780(c)-(d)
3. The witness's ability to remember. Evid. Code § 780(c).
4. The accuracy of the witness's communication of what he perceived. Evid. Code § 780(c). "Isn't it a fact that when you said that you were coerced, all you meant was that my client asked you to do it?"

38. What are the three rules for forensics hashes? How can we obtain digital hash?

“A unique numerical identifier that can be assigned to a file, a group of files, or a portion of a file, based on a standard mathematical algorithm applied to the characteristics of the data set. The most commonly used algorithms, known as MD5 and SHA, will generate numerical values so distinctive that the chance that any two data sets will have the same

hash value, no matter how similar they appear, is less than one in one billion. ‘Hashing’ is used to guarantee the authenticity of an original data set and can be used as a digital equivalent of the Bates stamp used in paper document production.