INSTITUTO SUPERIOR TÉCNICO

DEPARTAMENTO DE ENGENHARIA INFORMÁTICA

FORENSICS CYBER-SECURITY

MEIC, METI

Exam Solutions

2023/2024

nuno.m.santos@tecnico.ulisboa.pt

Contents

1 Exam 2 – 2022/23

I.

1. a. For internal investigations you need a signed letter of agreement outlining the scope of the investigation along with contractual details. For civil and criminal investigations you need a court order prior to starting.
   b. For instance: binds identity to integrity operation; prevents unauthorized regeneration of signature.
   c. No, these tools are meant for file carving not for steganalysis purposes.
   d. No; none of the admissibility evidences was in principle violated.
2. a. Disagree. First move the mouse to turn on the screen and then decide what to do.
   b. Agree. It was well done to use this window of opportunity, and the procedure was technically correct.
   c. Agree. Otherwise continuity of possession would be undermined introducing a gap in the chain of custody.
   d. Disagree. It would also be necessary to store the hash of the image!

II.

1. E.g., much less intrusive, has access to the whose physical memory.
2. a. Only F.
   b. From X_0 and X_1 we infer that this version can detect nested files.
   c. The pass was made from right to left.
3. (1) yes; protection enforced by the disk controller, data is not encrypted. (2) no: data is encrypted on the disk. (3) no: SSDs have no platters.
4. a. Output the contents of a file based on its inode number.
   b. It's an index to the MFT table.
   c. The content itself of the MFT!
5. For example: UserAssist, LastVisited MRU, RunMRU / Start->Run, Jump Lists, Prefetch, Service events
6. Disk B, because chances of fragmentation are much higher.
7. a. Signature based
   b. The mail server is infected by the botnet and is being used for performing ping sweeps
   c. IP1: 10.0.1.8 $\rightarrow$ 0a.00.01.08, IP2: 10.0.1.21 $\rightarrow$ 0a.00.01.15, IP3: 10.0.1.40 $\rightarrow$ 0a.00.01.28, IP4: 10.0.1.128 $\rightarrow$ 0a.00.01.80.
8. For instance, real-time monitoring and analysis of events; tracking and logging of security data for compliance or auditing purposes

III.

1. a. F, b. F, c. T, d. T., e. F, f. T, g. F, h. F
2. a. The destination; it will force the deauthentication of the destination.

b. Perform similar query but filtering based on the source address – the attacker's – and checking if the destinations correspond to the MACs of other victims.

c. Ask for IMEI/IMSI records of mobile stations connected from the airport in said period to identify potential suspects, possibly just one; then go to the field and locate it using an IMSI catcher or simply wait to be attacked. If you receive a deauthentication frame you will be very close to the attacker.

3. a. Cookies can immediately be used to let the attacker access the user account!

   b. Flush the cookies from the database forcing users to re-authenticate on the website.

4. Not even a bit: the rendezvous point cannot tell the IPs of client and hidden service.

5. a. Static. The code is not executed.

   b. For example, execute and hide a backdoor.

6. a. No. Shared preferences are key-value xml files, not file caches.

   b. Yes, Chip-off involves heating the device's circuit board until the solder holding the components to the board melts, and then removing the flash memory chip. JTAG requires only opening the device and attach wire to the JTAG interface.

2 Exam 1 – 2022/23

I.

1. a. Some of these: define the scope and likely venue of the examination, identify the stakeholders, identify the likely sources of evidence for the case, identify the forensic tools required, identify the personnel needed, collect all needed legal documentation.
   b. No, as long as he gets a new warrant.
   c. Inculpatory: evidence that supports a given theory. Exculpatory: evidence that contradicts a given theory.
   d. (1) validate the soundness of the results, (2) promote the reproducibility of the results.
2. a. Disagree. He didn't use write blocker, so we don't know if the integrity was compromised or not.
   b. Disagree. He should have bootstrapped the laptop from the USB drive in the first place.
   c. Agree. Otherwise continuity of possession would be undermined introducing a gap in the chain of custody.
   d. Disagree. This would have created logical copies.

II.

1. ICMP flood => 185.15.58.226
2. A is a virtual address, which means it cannot be used directly as an index to the physical memory dump. It first needs to be translated with the help of the process page table.
3. a. No, we would need to know the full size of the partition, which is not provided.
   b. By analyzing the inode bitmap and the block bitmap.
   c. Locate the root directory's inode, visit the corresponding inode in the inode table, obtain the pointed blocks, and dump their respective content.
4. (1) no fragmentation
5. He's using an alternate data stream to hide the secrets inside file cmd.ext. To detect, list the ADSes of all files in the system.
6. MAC address
7. a. Pings
   b. Machine with IP 192.168.1.35 is performing a ping sweep; found two machines: 192.168.1.27 and 192.168.1.27.
   c. The IDS server is probably compromised.
8. IP1: 146.193.41.40, IP2: 193.136.128.169, IP3: 172.16.1.3, IP4: 185.15.58.226

III.

1. a. F, b. T, c. T, d. F., e. T, f. F, g. F, h. F
2. Good: More robust to signal interference in densely populated areas. Bad: Needs effort and money for constant field monitoring and updating of the radiomap.
3. a. ? -> mail-pf1-x444.google.com -> smtp1.tecnico.ulisboa.pt -> mail2.tecnico.ulisboa.pt

b. It has one frontend smtp server that forwards the emails to one of two possible backend servers: mail1 or mail2.

4. Dynamic analysis

5. a. C -> Entry Relay / Guard -> Middle Relay -> Exit Relay -> S
   b. Latency will improve. Less time to look up DNS.
   c. Will seriously compromise anonymity. The ISP of the client will immediately the destination IP that the client is intending to access.

6. a. true
   b. false

3 Exam 2 – 2021/22

I.

1. a. T, b. F, c. F, d. F., e. T, f. F, g. T, h. F
2. Legality no: cannot copy the email of everyone. Everything else pretty reasonable.
3. a. (2): it's the very purpose of this command. (1) lists open network connections. (3) dumps 2KB of memory.
   b. Not necessarily. In theory, depending on the setup and the commands performed by the analyst, is possible to inspect the system state in such a way that only the volatile state is changed.

II.

1. a. Targeted steganalysis: Relies on knowing the method used to hide the data & using known distinguishing statistics to detect stego images. Blind steganalysis: it's not based on knowing the algorithm, more difficult.
   b. For instance, identify a signature pattern related to the steganography program.
2. Fully: C,D ; Partial: A,E ; Unsuccessful: F,B.
3. Acceptable: Leverage a kernel driver / module to access physical memory without restrictions.
4. a. The icat tool allows you to view the contents of the data units that are allocated to a metadata structure, in this case inode 69457.
   b. The returned content seems to be structured in the form of a list of file names, this suggests that the file pointed to by inode 69457 is likely a directory.
5. No. This would be incomplete. The registry database is only ever complete when loaded into your computer's memory.
6. Packet sizes.
7. a. Use an IP geolocation service to determine the location of the owner of the IP address 176.31.84.249, e.g., whois.
   b. 192.168.30.52
   c. At least two things: 1) types of packets being transmitted, no longer TCP syn-enabled packets, but ICMP packets, 2) scan not a single destination IP, but multiple IPs within the local network.
8. By the proximity to the closest stations.

III.

1. a. PHP injection vulnerability reusing a debug function that may have caused the deletion of data from the database.
   b. Nothing in Ana, in Bruno's email something to click on a link to https://intranet.gs.pt/patient.php?req=0;debugResetDB()
2. Example 1: Dynamic (server generated) web pages and searchable databases; Example 2: Unlinked contents, for instance, pages without any links to them (orphan).
3. A - destination anonymity, B - sender anonymity, C - no anonymity, D - no anonymity

4. a. DDoS, click fraud, spamming campaigns, etc.
   b. Manages the entire botnet network membership, and coordinates the execution of large scale attacks as instructed by the botnet master.
   c. Hide the location of the command and control server.

5. static: a, b, c; dynamic: d

6. 1) can track all the transactions performed by the real person, and 2) can move the money from the person's account.

7. a. False, internal storage is non-volatile flash memory.
   b. True, hinders accessibility (also ok to say that battery is drained).

4 Exam 1 – 2021/22

I.

1. No. The Kruse model is incomplete. For instance, it does not fully specify the terms in which a digital artifact might be considered relevant or irrelevant for a given case. But most importantly, admissibility ultimately is decided by the judge.

2. a. 1) If power supply is interrupted, 2) how fast data changes.
   b. t2 because it gives precedence to artifacts that are more volatile.

3. a. Correct. In this case the scope of the investigation is confined to the organization. This is an internal investigation.
   b. Incorrect. Too disruptive for the organization, and in reality most evidence – if it exists – can be found in the logs themselves.
   c. Incorrect. The workstation is running and it is unlocked. This is a unique opportunity to collect evidence from the system.
   d. Incorrect. Since the device is rooted, you can connect using an ADB bridge and create a bitstream copy of the internal storage.

II.

1. a. p0 = 5 $\rightarrow$ ab86, p1 = 6 $\rightarrow$ 61a1, p2 = 7 $\rightarrow$ 0a16, p3 = 8 $\rightarrow$ 464b, p4 = 9 $\rightarrow$ 5de2
   b. Hint: yes, yes.

2. 1) Dumps the first 1GB segment of RAM memory to file file.dd, calculating also the hash and logging errors. 2) Method for memory acquisition: drawback e.g., requires admin privileges on the system, requires the previous installation of the fmem driver.

3. a. Master File Table
   b. In NTFS, the equivalent to an Extx inode is an MFT entry. Therefore, x is likely the MFT entry of the file in the MFT table. Besides, apart from the two first lines, x is always different which is compatible with the hypothesis that there's one MFT entry per file. The second line is in fact an ADS of the same file.
   c. The number of $DATA in the MFT entry of the file. The second line shows an ADS of the first file # 40.
   d. It is a prefetch file. Prefetch files contain a history of the past execution of the program explorer.exe.

4. For instance, the sequence of bits signaling the footer of a JPEG file may exist in the body of a JPEG file.

5. 1) the MAC can tell you proximity: if you can negotiate with an AP with unknown MAC then you know you're close. 2) the MAC also give a hint of the AP model.

6. a. IP1: 207.148.248.143, IP2: 192.168.1.14, IP3: 192.168.1.8
   b. The public IP address of the gateway.
   c. Nothing. The rule is misleading. Every single TCP syn message will trigger an alert.

7. Netflow logger. It's impractical to store the packets for such a large amount of traffic.

III.

1. a. F, b. F, c. F, d. F., e. T, f. F, g. F, h. T

2. Sender of the email, network path it traversed and path of origination, SMTP servers it went through, timestamp details, email client information, encoding information.

3. a. It is the IP address of the entry node of the first circuit connecting the rendez vous node.
   b. The exploit will send the list of files of the remote server. This is a code injection vulnerability.
   c. Yes. Craft an input that reads the local IP address of the destination, or to look up the IP address e.g., sending a request to https://whatismyipaddress.com/

4. E.g., prevent access to a file that the rootkit wants to hide.

5. a. All affected by malware because IP is public and all run the same OS version, therefore they are all exposed. The malware is attempting to connect to a C&C server, using fast flux IP rotation.
   b. The malware is employing defensive techniques that disable external communications if running inside virtualized environment.
   c. Acceptable: If network logs exist see if there's evidence of exploits being delivered to the servers; on the servers themselves look for the process opening the connection, compare if similar process is running on different servers.

6. a. They merge the their money in a single account so that the analyst doesn't know who bought which asset. note: they both must transfer 0.2 BTC to a common account otherwise the analyst could tell who's buying each.
   b. Shared spending tries to associate two source accounts to the same person when those accounts are involved in a transaction. Fresh-change-address tries to associate the account of the change in a transaction with one or multiple source accounts.

5 Exam 2 – 2020/21

I.

1. a. Hint: violation of the relevance guideline.
   b. Example: business records, and computer- generated data.
2. $m1$ can reveal more data than $m2$.
3. Consider the following investigative scenario:
   a. For instance: Ask the root password to the sys admin, then create a full disk image from the mail server / create a logical image of the email files and logs.
   b. For instance: Power off the server. Bring the disks to the lab because they are very big. Create a bitstream image of each disk. Do forensic analysis.
   c. For instance: Pull the plug immediately to prevent further destruction of evidence. Boot the system from a forensically sound OS, create disk image in the spot and bring it to the lab.
   d. For instance: Check what's going on and see what kind of activity is taking place. If it's data exfiltration, immediately disable the wireless network card. Other explanations might be acceptable. Then create a disk image.

II.

1. 1440 x 1080 x 3 / 4
2. a.

File	Single-pass structure-based carving tool	Bifragment gap carving tool
A	A_0	A_0
B	B_0, C_0, C_1, D_0, D_1, C_2, $-$, E_0, E_1	B_0, B_1
C	$\times$	C_0, C_1, C_2
D	$\times$	D_0, D_1

   b. No. It's the other way around: C is fragmented around D.
3. First, locate the Linux kernel data structures that contain the page directory of each process, then for each page directory, navigate through the page tables of each process and save the contents of each page in a separate file.
4. a. Hint: No.
   b. Hint: Yes.
   c. Hint: No.
   d. Hint: True.
5. Example: RunMRU, Last Visited MRU
6. a. Hint: Brute force attack.
   b. Hint: Yes.
7. For example, two of these: (1) Search for common binary/hexadecimal/ASCII values that are typically associated with a specific protocol, (2) Leverage information in the encapsulating protocol, (3) Leverage the TCP/UDP port number, many of which are associated with standard default services, (4) Analyze the function of the source or destination server (specified by IP address or hostname), (5) Test for the presence of recognizable protocol structures.

III.

1. a. F, b. T, c. F, d. F., e. F, f. T, g. F, h. F
2. a. Hint: 41.32.28.249
   b. Hint: HTTP.
   c. Hint: No.
3. For instance, backdoors and hiding utilities.
4. The private keys of the bitcoins accounts.
5. a. Hint: dynamic.
   b. For instance, scanning for files containing interesting data in well known locations.
   c. E.g., set up an isolated virtual machine.
6. Anonymization of the destination IP address.
7. For example, WAPS (a) may contain locally stored logs of connection attempts, auth successes and failures, and other local WAP activity, (b) can help track the physical movements of a wireless client throughout a building or campus.

6 Exam 1 – 2020/21

I.

1. a. T, b. F, c. T, d. F., e. F, f. F, g. F, h. T
2. a. Possible responses: Yes. To prevent further spreading of the malware. / No. May result in losing evidence and the possibility to recover the encrypted data
   b. Possible response: No. We don't want to lose the volatile state, e.g., keys that will allow us to decrypt the data.
   c. Possible response: Yes. To recover the decryption keys in memory.
   d. Possible response: No. E.g. we can track email, monitor traffic, etc.

II.

1. p0 = 9cb0, p1 = d163, p2 = 705b, p3 = 8787
2. For example: tree/list traversal can miss unlinked, dead structures; fingerprint/pattern search is susceptible to rubbish.
3. a. Hint: NTFS
   b. The content of the file associated with attribute $DATA is stored in a set of clusters pointed out by the output, e.g., 10016, etc.
   c. The four indirect blocks indicated by the output (14392, etc.) contain references to blocks containing actual file contents.
4. Acceptable: (a) superreg: read the Internet browsing history and search for websites known to distribute child pornography; (b) bicarv: recover deleted images / videos of child pornography.
5. Acceptable: Yes. Timestompers cannot update the timestamps with sufficient granularity resulting in the assignment of zeros in the least significant bits.
6. Hint: infected system attempting to connect back to a command-and-control channel.
7. Explain in what way the two middleboxes below complicate the analysis of network traces:
   a. NATs hide multiple clients behind the same IP address. Hard to tell who the sender is.
   b. Traffic is encrypted. Hard to tell the remote destination if intercepting the traffic between client-VPN server; hard to tell the source if intercepting traffic between VPN server-destination.
8. For instance, two of these: (a) can't inspect encrypted traffic (VPNs, SSL), (b) can't record and process huge amount of traffic, (c) high false positive rate, (d) false negatives: attack is not detected.

III.

1. Hint: attempt to launch a spear-phishing attack.
2. Hint: Alice-R1 and R3-CNN.
3. Hint: Fast flux. DGA. Encryption. P2P architectures, etc.
4. a. The number of processes should be the same. Suggests an attempt to hide a process. Typical of rootkits.

b. Hint: file masquerading.

c. E.g., check open ports, dump an image of the hidden process, analyze the ps file though hashing and other static analysis techniques, etc.

5. Shared-spending heuristic.

6. IMSI is stored in the SIM card and can be used to identify the subscriber of the network provider's service.

7. a. E.g., difficult to remove internal storage, locking mechanisms, dependent on power supply, network connectivity which may compromise the integrity of the data, etc.

   b. For instance, strength: can access the full persistent state of the device; Weakness: complex, requires specialized hardware, damages the device.

   c. Key-values used by many applications, sometimes even storing usernames and passwords.

7 Exam 2 – 2019/20

I.

1. a. Assessment, acquisition, analysis, reporting
   b. Temporal, relational, functional
2. Hint: Produce the same output when given the same rule set and input data
3. a. Hint: Shut it down. Boot forensic OS and create image. Or bring the hard disk to the lab.
   b. Hint: Don't power up the server. Bring the disks to the lab because they are very big.
   c. Hint: It might be possible to recover the files from the unallocated disk space. Create disk image in the spot, or bring the hard disk to the lab. Disk is small / you have the root pass, so both are acceptable.
   d. Hint: Disconnect the network cable. Log in quickly. Check what activity was taking place and collect what you can. This can give you also access to memory. It might also be acceptable not to disconnect the network, if the argument is that destruction or data transfer was not being carried out.

II.

1. 1600 x 1200 x 3 x 2
2. a.

File	Single-pass structure-based carving tool	Bifragment gap carving tool
A	A_0, A_1, A_2, F_0, F_1	A_0, A_1, A_2, A_3
B	B_0, D_1	B_0, B_1
C	C_0	C_0
D	D_0, E_0, E_1, $-$, E_2	D_0, D_1

   b. Yes. A is fragmented around F.
3. Hint: list of running processes, list of open network connections
4. a. Hint: No. It's independent of the underlying technology because the CHS addressing scheme is obsolete. However, also accept yes, if there's some mention to the CHS addressing scheme, which of course is dependent on the disk geometry.
   b. 3 partitions: Linux, NTFS, Linux
   c. Hint: It is used to retrieve the first partition.
5.
6. a. Hint: Port scan that consists in sending TCP packets with SYN flag set and wait for response with the SYN/ACK or with a RST message.
   b. Hint: The traffic suggests port knocking. Probably the server is infected by backdoor and port knocking is used to conceal the backdoor port.
7. Hint: It's a kind of phishing attack targeting a specific employee within the organization. Check evidence from the employees' email.

III.

1. a. T, b. F, c. T, d. T., e. F, f. F, g. T, h. F

2. a. Hint: Periodic HTTP requests coming from local computers toward some external server, possibly multiple ones.
   b. Hint: No. Drive-by-download is a matter of exploiting vulnerabilities in the browser. Strong passwords don't help.
3. Hint: They can interfere with the normal functioning of the operating system, e.g., by hooking into the system call vector.
4. Hint: For example, sniffing the traffic between the user's Bitcoin client application and the Bitcoin system and match the IP address of the client and the public key of the transactions issued from that client. This is possible because the Bitcoin protocol is not encrypted.
5. a. Static: it extracts all the strings from the executable without running the program
   b. Hint: The ASCII strings extracted from the malicious binary show reference to an IP address. This indicates that when this malware is executed, it probably establishes a connection with that IP address
6. Hint: Examples: simple eavesdropping on the exit node, send fake certificates in order to intercept HTTPS traffic
7. Hint: information about the cell where the device is connected to.

8 Exam 1 – 2019/20

I.

1. A fundamental goal of digital forensics is to produce admissible evidence.
    a. Relevant, authentic, credible, collected legally
    b. Possible answers: dynamism of the system, guarantee completeness, etc.
2. Hint: Advantages: The device continues running and temporal data remains intact. Disables cellular data net and WiFi. Disadvantages: You are modifying the device setting further. Only works if you have full access to the device.
3. a. Hint: Evidence suggesting the extraction of sensitive data from the file server to the suspects' computers, and from there to the remote computer. For example, ssh logs, netflow traces, copies of files in the suspects computers.
    b. Hint: Image of the hard drive; unplug from the network / power off the computer, then boot the system into forensically sound OS and create an image to external hard drive, calculate hashes, etc.
    c. Hint: Image of the hard drive; don't reboot because the disk might be encrypted, create an image to external hard drive, calculate hashes, etc.
    d. Hint: ssh logs of file server, netflow system, and VPN; collect the respective files from each server by requesting credentials from the sys admin, calculate hashes, etc.

II.

1. Hint: structural detection, statistical detection, visual detection.
2. a. Structure-based carving: D, Content-based carving: A, Bifragment gap carving: B, C, e D.
    b. Yes. Look at the page tables of each process and see which pages are allocated to each process.
3. a. Means that the inode is not currently allocated to a file. Likely belongs to deleted file.
    b. Deletion timestamp prior to other timestamps. 5184 repeated.
4.
5. a. source IP: 139.133.217.111 => 0x8b85 d96f; destination IP: 0x92c1 2928; destination port: 0x1F90 (8080); Flags = 0x02
    b. Syn flag is set. Probably DDoS attack with sender IP spoofed.
6. Acceptable: i) port scans: target same ip different ports from same ip, ii) ping sweeps: ICMP packets, target range of different IPs, from the same ip
7. No, because they can be fully consistently and completely fabricated.

III.

1. a. T, b. F, c. F, d. F., e. T, f. F, g. T, h. F
2. a. Hint: Likely to be a botnet's Domain Generation Algorithm
    b. E.g., collect a sample of the malware from the source of this traffic

3. a. Hint: The coast is clear: you can read the transaction records and public keys associated with Mr. Black's accounts; you can even follow through by checking transactions in the Bitcoin ledger based on his public keys.

   b. Hint: There's not much you can do. No access to the application state, no access to public keys nor transaction records.

4. a. Hint: i) static analysis: safer, ii) dynamic analysis: can be more efficient

   b. Hint: i) static: code obfuscation, ii) dynamic: detection of virtualization / debuggers

5. Hint: no, it's the rendez-vous node of the hidden service

6. Hint: yes, for the files whose data attribute has been marked to be resident, which is the case for the small-sized files that can fit inside an MFT entry

9 Exam 2 – 2018/19

I.

1. Possible answer: entries in the web server log, URL history on the desktop.
2. Hint: One way hash functions are cryptographically stronger.
3. Hint: The volatility level depends on whether: A consistent power supply is required for storage. How fast data changes.
4. Hint: Authenticity no: no integrity checks of the obtained copies.
5. a. E.g., in identifying the most likely sources of evidence based on the nature and circumstances of the crime (crucial in large networked systems).
   b. Hint: Rigidness: In practice, most digital investigations do not proceed in linear fashion.

II.

1. a. T, b. F, c. T, d. T., e. F, f. F, g. T, h. F
2. LSB-3
3. For example: i) User level applications: Good for incident scenarios, for capturing forensic image even in situations with little time. ii) Kernel level applications: Can access physical memory without restrictions. iii) Dedicated hardware card: Beneficial when installed on critical servers.
4. Hint: Timestamp of X.avi seems inconsistent: it it were correct, it should have appeared in the snapshot of Jan 19th, which does not. Furthermore it exhibits signs of tampering by having zeroed list significant timestamp digits. So, we cannot trust it. However, we know that X.avi has overwritten B.doc hence, it must have been downloaded after B.doc. Since the timestamp of B lesser than A's it suggests that Smith first has deleted B and then edited A. Now, both things might have happened: X could have been installed after B's and after A's modification – being consistent with Mr. Smith's story; or X could have been installed before A's modification, but we cannot determine that. So both hypotheses are possible.
5. Hint: An internal computer with IP 192.168.30.101 is performing a site scan for any Web servers (port 80) located in the internal network. Perhaps the sender has been compromised by an attacker who's using that computer as a pivot for compromising other internal systems, e.g., an intranet server.

III.

1. a. Hint: R3 because it is encrypted with R3's key.
   b. Hint: The middle node because it contains another encrypted message to one last relay before arriving B.
2. Hint: Can send millions of synchronized packets to a victim.
3. a. Hint: Dynamic analysis. Need to run the program.
   b. Hint: It's opening a socket and downloading content from IP 146.193.41.139. Maybe to obtain a list of updated servers for future communication.
4. Hint: Yes. Match the IP with the signatures issued by the client for the submitted transactions to the Bitcoin network. This is possible because the communications are not encrypted.

5. Hint: i) check IP of sender's email 188.140.58.213 is owned by the mobile carrier, ii) then check at the time of the sending of the message Wed, 23 Jan 2019 10:42:00 -0800 (PST) who owned that IP, iii) IP associated with client that owned the IMSI used by smartphone to join the broadband network, iv) IMSI identifies the subscriber ID, who has a contract, so we can know it's Ken and it's address

6. Hint: Decompile the DEX bytecode. Modify the resulting code in order to (1) inject the Trojan, and (2) remove integrity checks. Recompile the application. Sign it with the attacker's private key. Create apk package

7. Hint: Indicate respectively which inodes and blocks belong to allocated files.

8. a. Hint: Yes because it's a resident file. Had it been non-resident, we would have had to parse the run list and locate the clusters in the file system image.
   b. Hint: Yes, because only has one $DATA attribute.
   c. Hint: Cannot tell that simply by looking at the MFT entry.
   d. Hint: No. Had to do strides of 1024 because each entry of the MFT has fixed size of that value.

10 Exam 1 – 2018/19

I.

1. Possible answer: interaction with computer systems causes state changes, things you leave and things you bring

2. a. Hint: state integrity not entirely preserved.
   b. Hint: server cannot be shutdown, relevant data in memory.

3. a. Hint: Internet history, local documents, bitcount wallets, etc.
   b. Hint: main problem is if the data on disk is encrypted and relevant volatile memory (e.g., windows registry). Don't turn off the computer. acceptable answer: make disk image w/o unplugging the computer, dump content of the registry from memory. Store evidence in forensically sound device, create hashes, update the chain of custody.
   c. Hint: plug the device to the power supply, extract the data logically over usb to the forensic station on spot, take the device, store evidence in forensically sound device, create hashes, update the chain of custody.
   d. Hint: explain how actions help to introduce least state changes, mention MD5, and chain of custody.

II.

1. Hint: List traversal: +) Can stitch together more related records from kernel perspective, -) Can miss unlinked, dead structures, targeted countermeasures.

2. 62 + 1542240 + (7000000 - 6265349 - 1)

3. detects nested headers (lines 6-9)

4. Hint: prefetch exist in windows machines so we exclude Claire; then check the prefect file associated with sftp tools on Alice's and Bob's desktops to see if it was executed at that time; depending whether you find evidence of execution around that time need to proceed further to collect more evidence on that specific desktop.

5. Hint: Signature-based analysis, behavioral analysis.

6. Hint: buffer overflow exploit.

7. a. IP of A: 0x92c1 29c9, IP of B: 0x92c1 290a, IP of R: 0xc188 806e
   b. Data region not a regular ping. Maybe a covert channel to exfiltrate data using optional data region.

8. Hint: Look for breaks / discrepancies in the "Received" lines; Verify all IP addresses: Keeping in mind that some addresses might be internal addresses; Make a time-line of events. Change times to universal standard time. Look for strange behavior. Keep clock drift in mind; etc.

III.

1. a. F, b. T, c. F, d. F., e. F, f. F, g. F, h. T

2. Hint: For example, a command-level rootkit

3. a. Hint: 0.1 + 0.1 + 0.05 = 0.25 (use change heuristics to obtain these values; cannot go beyond with transfers involving Alice 1, because Alice 1 is not deanonymized)

b. Hint: 0,55 (using shared spending heuristics, and account ID of Alice associated with Bob's transaction.)

4. Hint: Only c would work.

5. Hint: No, because you can correlate traffic at both endpoints.

6. a. First cluster: 140f, then: 1409, 1415, 1417. Total, 4 clusters
   b. Size of file 2: 0x600 bytes < cluster size = 0x800 bytes. So yes.
   c. No because file has been deleted but the cluster has been allocated to another file (EOF symbol on FAT entry 0x1413)

11 Exam 2 – 2017/18

I.

1. a. F, b. T, c. T, d. F., e. F, f. F, g. F, h. F
2. a. Hint: No. Need chain of custody too.
   b. Hint: Yes. Looking primarily for evidence on the disk.
   c. Hint: No. Need to use several file carvers.
   d. Hint: No. Need to tell that to authorities and start a new investigation.

II.

1. Hint: get some images, use a sample string, apply the tool to those images, inspect which bits have been altered.
2. Hint: If rooted, user data partitions can be mounted read-only and use imaging tool, Backups, JTAG interface, Chip off.
3. Hint: Dedicated hardware card: Limitation: prior installation of PCI card before its use, Beneficial when installed on critical servers. Crash dump: Practical, more invasive.
4. Hint: both file name structures will point to the same metadata, so you can't tell what was the last file name associated with the metadata entry.
5. Successful: B ; Partial: A, F, and D, Unsuccessful: E,C.
6. Hint: Look for magic numbers and other data structures of the file system.
7. Hint: The $DATA attribute: the first has 2 attributes, the second has only 1.
8. Hint: Userland hooks in the Import Address Tables (IAT), The Interrupt Descriptor Table (IDT), The System Service Dispatch Table (SSDT), Device drivers via I/O Request Packets.

III.

1. Hint: When you see multiple entries associated with a particular hop, it means there are multiple pathways at the same net distance to the destination.
2. a. Hint: destination IP: 139.133.233.2 => 0x8b85 e902, destination port: 0x17, flags = 0x10.
   b. Hint: ACK scan because the flag is set.
   c. Hint: If network has firewall with Stateful Package Inspection (SPI) ACK will be quietly discarded.

3 a. 1 - 00:22, 7 sec, 3755 bytes; 2 - 00:29, 7 sec, 3755 bytes; 3 - 00:35, 7 sec, 4603 bytes; 4 - 00:41, 7 sec, 3755 bytes
   b. Hint: Someone is trying to periodically access the server, e.g., experimenting different passwords. Eventually it seems to have succeeded because the flow size has changed, and flows stopped.

4 Hint: Gather station descriptors, Identify nearby wireless access points, Signal strength, Commercial enterprise tools.

5. a. Hint: 194.210.220.81 -> max.mpi-klsb.mpg.de -> juno.mpi-klsb.mpg.de -> mail.inesc-id.pt -> mail.gsd.inesc-id.pt
   b. Hint: The clock of mail.gsd.inesc-id.pt is incorrect by -3 hours.
6. Hint: B. He can correlate traffic from both endpoints.

12 Exam 1 – 2017/18

I.

1.

2. a. Hint: Prevent writes to storage device. SW that interposes between driver that blocks write instructions to the block device.
   b. Hint: dd obtains bit-steam image, thus more information; cp only file contents and some metadata.

3. a. Hint: logs in the server at least, activity in the suspect's workstation.
   b. Hint: server live analysis, logical file copy, MD5; create disk image without rebooting the machine, MD5; chain of custody.
   c. Hint: Relevance: only collected what was relevant for the case; Authenticity: MD5 and chain of custody; Credibility: logs ok; Legality: had proper authorization

II.

1. Hint: Hidden message: 01100101 vs. 01100001 => 7 bits overlap => watermark detected.
2. Hint: Dirt / deformations, Lens distortions, Pixel defects.
3. Hint: PUP: Errors propagate in cascade, still slow in practice; BGC: It only works for files of two fragments, it only works for files that can be validated, correct validation does not mean coherent/correct.
4. Hint: In the master file table entry of the file, it's small enough that it can fit in the entry.
5. a. Hint: 14 blocks.
   b. Hint: file slack = 0x1000 - 0x0002 bytes
   c. Hint: no, because direct entries 2 and 12 point to the same block.
6. Hint: Prefetch: no, just for executables; LNK files: yes, may point to deleted files; Shell Bags: unlikely because keeps track of recently opened directories; Recycle Bin: yes for obvious reasons; Run MRU: unlikely because it keeps track of most recently executed programs from the start menu.

III.

1. a. Hint: sql injection to retrieve the data
   b. Hint: the ip of the source actually correspond to the same network, it's an insider job, browser type.
   c. Hint: obtain authorization, see if there is dhcp, to determine who's launching the attack, go talk to the responsible.

2 Hint: No. Port knocking may be in use.

3. Hint: Any two of the following: RIR databases, Probe data sources where IP address has shown up before, ISPs may also may contribute information to databases, Parsing reverse-dns (PTR) records looking for clues.
4. Hint: A: possibly http browsing session, B: tor browsing session (fixed cell size), C: streaming a video for example over http or other protocol.

5. Hint: Strengths: i) Bitcoin address are not mapped to the real user identity, i) Bitcoin transactions don't contain personal information, iii) IP address of client not included in new transactions, iv) User can generate as many Bitcoin addresses as needed. Weaknesses: i) Authentication mechanism in Bitcoin service providers may link user IPs to Bitcoin addresses, ii) The chain of transactions is transparent and traceable, iii) Bitcoin address exposed on the Internet reveal all transactions related to its owner, iv) Gathering some or all inputs when sending Bitcoins to others may expose other addresses of the sender.

6. a. F, b. F, c. T, d. F., e. F, f. T, g. T, h. F

13 Exam 2 – 2016/17

I.

1. Hint: No. Didn't take anything with him.
2. Hint: Authenticity não: no chain of trust.

II.

1. a. F, b. F, c. T, d. F., e. T, f. F, g. T, h. F
2. Hint: When powered on, the device announces itself to the network, starting the authentication process. The authentication process is based on the IMSI. Identity Mobile Subscriber Identity (IMSI) is a unique # stored on the SIM card and associated with a particular subscriber. IMSI is not directly sent over the network, but replaced with a Temporary Mobile Subscriber Identity (TMSI), which is logged. Investigators can ask NSPs to query their systems for all activities relating to a particular subscriber account.
3. a. Hint: NTP
   b. Hint: DHCP is delayed by 18:21 - 15:21 hours = 3 hours.
   c. Hint: Lease 1 start: 5:35 + 3:00 = 8:30; Traffic start: 12:01; Traffic stop: 12:03; Lease 1 stop: 9:35 + 3:00 = 12:30; Lease 2 start: 11:09 + 3:00 = 13:09; Lease 2 stop: 15:09 + 3:00 = 18:09. A is the culprit.

III.

1. a. 2 partitions: Linux, NTFS
   b. P1: 0x3FFFFF x 512 => 2GB - 512 bytes, P2: 0xA00000 x 512 => 5GB
   c. P2: 5GB (0xA00000 sectors) and starts at address 0x800000 x 512 => 4GB. Volume size is 8GB. Therefore, P2 is out of bounds (by 1GB).
   d. Hint: Yes. Start: sector 0x400000 (2GB), size: 0x200000 (1GB). Entirely between: P1 < 2GB - 3GB-1 < P2
2. Hint: JTAG interface: used during the device production process to communicate with the processor for testing. Allows examiners to communicate directly with the processor and retrieve a full physical image of the flash memory. Chip-off involves heating the device's circuit board until the solder holding the components to the board melts, and then removing the flash memory chip. The memory chip can then be read using commercial tools, resulting in a full physical image.
3. Hint: Structure-based carving: D, Content-based carving: A, Bifragment gap carving: B, C, e D.
4. Hint: a. Search for common binary/hexadecimal/ASCII values that are typically associated with a specific protocol. b. Leverage information in the encapsulating protocol. c. Leverage the TCP/UDP port number, many of which are associated with standard default services. etc.
5. Hint: Signature-based analysis: Oldest strategy; compares contents of packets, and streams of packets against databases of known, malicious byte sequences in order to identify suspicious traffic. Protocol awareness: Detect malformations in network protocols by checking if packets conform to RFC specifications; may require reassemble fragments (Layer 3), flows (Layer 4), or entire app protocols (layer 7). Behavioral analysis: Using a model of normal system behavior, try to detect deviations and abnormalities, e.g. trigger alert if incoming traffic volume increases above certain threshold.

6. Hint: By analyzing the Received field, we see a gap in mail path: nercomp => prod3 => mi24 => MISSING => o1 => krait => BFRANKLIN04

IV.

1. Hint: It depends. If the proxy is connected to the IST, no. Otherwise, yes.
2. a) Hint: 7 + 2 = 9 Bitcoin
   b) Hint: No. One output goes to the same account. Seems like a regular transaction with a different user.
   c) Hint: Yes. Shared spending.
   d) Hint: Yes. Closed graph.
3. Hint: Only effective for file masquerading, and under the condition that the integrity checkers have not been compromised.
4. Hint: Reserved region on hard disks that are used for storing manufacturer-related information and accessed through the ATA / SCSI interfaces.
5. 48MBit
6. Hint: Removal attacks, geometrical attacks, cryptographic attacks, protocol attacks.

14 Exam 1 – 2016/17

I.

1. a. F, b. T, c. F, d. F., e. F, f. F, g. T, h. T

II.

1. Hint: The scientific method aims to overcome the following limitations of investigation models: (a) complexity (define many steps and cumbersome inter-relations), (b) rigidness (in practice, most digital investigations do not proceed in linear fashion), (c) incompleteness (don't help digital investigators with some of the most important steps of each step of an investigation, including the completeness and repeatability of each step).
2.
3. Hint: Use browser fingerprinting techniques.
4. a) Hint: No. C overlaps D.
   b) Hint: Can't tell. Don't know if B overlaps D or vice versa.
   c) Hint: No. A is fragmented due to B.
   d) Hint: No. E occupies a sector immediately after A, which suggests A was already there before.

III.

1. a. 3 partitions: NTFS, Linux, and Linux
   b. P1: 0x1FFFFF x 512 => 1GB - 512 bytes, P2: 0x800000 x 512 => 4GB, P2: 0x400000 x 512 => 2GB
   c. Hint: P2 and P3 overlap; P2: 4GB and starts at address 0x800000 x 512 => 4GB; P3: 2GB and starts at address 0xC00000 x 512 => 6GB.
   d. Hint: 3 GB
3. Hint: Content: operate at the data unit abstraction layer, Metadata: operate at the file metadata abstraction layer. FAT: content - clusters, FAT; metadata - directory entries, FAT. NTFS: content - clusters, $BITMAP; metadata - $MFT, etc.
4.
5. Hint: Use the following tools:

Packet analysis tools	**Flow analysis tools**
t1: Pattern matching	t4: List conversations and flows
t2: Parsing protocol fields	t5: Export a flow
t3: Packet filtering	t6: File and data carving

   For example: use t1 and t3 to learn most of the information from events E1-E4; export the flow containing the file using t5; run t6 to carve the file. Etc.

IV.

1. I_1 => R1, I_2 => R2, I_3 => Bob, K_1 => R3, K_2 => R1, K_3 => R2, K_4 => Bob
3. Anonymity of the destination.

4. Hint: Shared spending heuristic: link transactions that belong to the same user. Can be used for deanonymization purposes.

5. Hint: P2P architectures, fast flux, and Domain Generation Algorithms (DGA).

5. Hint: p0 = 2d31 || 11 = 2d33, p1 = c5d8 || 11 = c5db, p2 = 2030 || 00 = 2030, p3 = 0a3c || 01 = 0a3d

15 Exam 2 – 2015/16

I.

1. Hint: Chain of custody, a.k.a continuity of possession: documents who has handled the evidence in order to ensure the authenticity of evidence.
2. Hint:
    1. Files were deleted by the user: look for malware and records in the registry that reveal traces of commands that deleted the files.
    2. File was copied to a USB drive and deleted afterwards: check that there are no log entries of USB drive connections.
    3. Files were deleted by another user: check that nobody has logged in the system in the interim of Alice's accesses.
3. a. 1, b. 4, c. 2, d. 3, e. 3, f. 1, g. 4, h. 4

II.

1. a. Hint: Size root dir = 512 * 32 / 512 = 32
    b. Hint: Total number sectors - system reserved area, system reserved area = 1 + (2 x FAT size) + root directory size
    c. Hint: Slack = volume size - total number of sectors
2. Hint: FAT16: check the FAT; Ext2: check block bitmaps; NTFS: check block bitmaps on MFT.
3. Hint: Journaling: transaction log of FS writes. Can be used to recover writes.
4. Hint: Self-wiping and self-encrypting drives.
5. Hint: Command-level: replace user-level programs; Library-level: replace system libraries. Approaches to detection, e.g.: 1. If a rootkit listens for connections, the network port will be visible to an external network port scanner, 2. Some tools can reveal the names of all directory entries, including hidden or deleted files, 3. Corrupted versions of ps and similar hide malware processes, but these can still be found using, e.g., the /proc file system, etc.
6. a. Hint: (1) unblock screen, (2) connect to power supply, (3) disable network interfaces, (4) copy password, (5) place device in faraday bag.
    b. Hint: Boot in recovery-mode and connect through ABD. Examples: SMSes, call history, apps, etc.

III.

1. Hint: a) yes, by checking large amount of flows from many different sources; b) and c) no, don't inspect the payload; d) yes, check for flows destined to well known ports for login.
2. Hint: Rotation of IP addresses. Observe traffic from a potential victim to many different IPs.
3. Hint: Check the cell where the device is currently advertising its presence. Use triangulation tecniques.
4. Hint: IMSI-catcher subjects the phones in its vicinity to a MITM attack, acting to them as a fake base station. Exploits GSM security hole where the network doesn't need to authenticate.

5. Hint: For example: use t2 to filter FTP traffic, then export the respective flow using t5, then run t1 to extract the username and password. Etc.
6. Hint: Yes.

IV.

1. Hint: Bifragment is more efficient
2. Hint: Hidden message: 11110001 => 0xF1

16 Exam 1 – 2015/16

I.

1. Hint: Assessment, Acquisition, Analysis, Reporting.
2.
3. a. F, b. T, c. F, d. F., e. T, f. F, g. F, h. F

II.

1. a.
   b. Hint: We can try to recover the file data by reading the data from the known starting cluster. A recovery tool (or person) has two options when it comes to choosing the remaining clusters to read. It can blindly read the amount of data needed for the file size and ignore the allocation status of the data, or it can read only from the unallocated clusters.
2. E.g., allocated DUs without an allocated file entry.
3. Hint: The MFT is the data structure that maintains all meta-data about NTFS file systems. It is used to keep track of allocated disk space and of existing files and directories in the system. The MTF is key to the recovery of forensic data about past activities involving the file system (e.g., recovery of deleted files).
4. Hint: An ADS consists of a secondary $DATA attribute that belongs to a particular file and can be used to hide data. It can be directly accessed using specific file system commands.
5. Hint: Challenge: garbage collection erases data in unpredictable ways; Opportunity: the wearing leveling algorithm creates replicas of data blocks.
6. Hint: E.g., in the Windows Registry

III.

1. Hint: SQL injection.
2. A: Hint: can correlate traffic based on timing.
   B: Hint: can correlate traffic based on timing.
   C: Hint: cannot correlate traffic.
   D: Hint: cannot correlate traffic.
3. Hint: Advantage: resilience; Disadvantage: latency.
4. Hint: Can't find any piece of content that is not reachable from an initial set of URLs. Overcome this limitation by randomly picking IPs and ports.
5. Hint: This is a syn flood attack. The SYN flag is set.

IV.

1. Hint: Successful: B; Partial: A and D, Unsuccessful: C.
2. Hint: Similarity: both embed a payload message on a cover message. Difference: steganography designed for security, watermarking designed for robustness.