TP4 RSI : Wireshark and network forensics

You are a forensic investigator and you have to investigates two scenarios. You possess the network capture (PCAP) file that was recorded when the problems occured. Your mission is to understand what happend and to give the evidences. Your analysis starts with the PCAP files and Wireshark.

First analysis :

Plot :

A company suspects that one of their employees, Ann D., is a secret agent working for their competitor. Ann has access to the company's prize asset, the secret recipe. Security staff are worried that Ann may try to leak the company's secret recipe.

Security staff have been monitoring Ann's activity for some time, but haven't found anything suspicious until now. Today an unexpected laptop briefly appeared on the company wireless network. Staff hypothesize it may have been someone in the parking lot, because no strangers were seen in the building. Ann's computer, (192.168.1.158) sent IMs over the wireless network to this computer. The rogue laptop disappeared shortly thereafter.

Questions :

1. What is the name of Ann's IM buddy?
2. What was the first comment in the captured IM conversation?
3. What is the name of the file Ann transferred?
4. What was the MD5sum of the file?
5. What is the secret recipe?

Second analysis :

Plot :

It is a morning ritual. Ms. Moneypenny sipped her coffee as she quickly went through the email that arrived during the night. One of the messages caught her eye, because it was clearly spam that somehow got past the email filter. The message extolled the virtues of buying medicine on the web and contained a link to the on-line pharmacy. "Do people really fall for this stuff?" Ms. Moneypenny thought. She was curious to know how the website would convince its visitors to make the purchase, so she clicked on the link.

The website was slow to load, and seemed to be broken. There was no content on the page. Disappointed, Ms. Moneypenny closed the browser's window and continued with her day.

She didn't realize that her Windows XP computer just got infected. Explain what probably happened to Ms. Moneypenny's system after she clicked the link.

Questions:

1. What was the starting URL of this incident? In other words, on which URL did Ms. Moneymany probably click?
2. As part of the infection process, Ms. Moneymany's browser downloaded two Java applets. What were the names of the two .jar files that implemented these applets?
3. As part of the infection, a malicious Windows executable file was downloaded onto Ms. Moneymany's system. What was the file's MD5 hash? Hint: It ends on "91ed".
4. What is the name of the downloaded malware ?
5. The malicious executable attempts to connect to an Internet host using an IP address which is hard-coded into it (there was no DNS lookup). What is the IP address of that Internet host?

Third analysis :

Plot :

After having been sent to jail for the leak the secret receipe, Ann Dercover is released on bail but then she disappears! Fortunately, investigators were carefully monitoring her network activity before she skipped town.

"We believe Ann may have communicated with her secret lover, Mr. X, before she left," says the police chief. "The packet capture may contain clues to her whereabouts."

As a forensic investigator, your mission is to figure out what Ann emailed, where she went, and recover evidences.

Questions :

1. What is Ann's email address and password for SMTP auth?
2. What is Ann's secret lover's email address?
3. What two items did Ann tell her secret lover to bring?
4. What is the NAME of the attachment Ann sent to her secret lover?
5. In what CITY and COUNTRY is their rendez-vous point?

Fourth analysis :

Plot :

While a fugitive in Mexico, Mr. X remotely infiltrates the Arctic Nuclear Fusion Research Facility's (ANFRF) lab subnet over the Interwebs. Virtually inside the facility (pivoting through a compromised system), he conducts some noisy network reconnaissance. Sadly, Mr. X is not yet very stealthy.

Unfortunately for Mr. X, the lab's network is instrumented to capture all traffic (with full content). His activities are discovered and analyzed… by you!

Questions:

1. What was the IP address of Mr. X's scanner?
2. For the FIRST port scan that Mr. X conducted, what type of port scan was it? (Note: the scan consisted of many thousands of packets.) Pick one: (TCP SYN, TCP ACK, UDP, TCP Connect, TCP RST)

3. What were the IP addresses of the targets Mr. X discovered?

4. What was the IP address of the Windows system he found?

Fifth analysis :

Plot :

Ann Dercover is after SaucyCorp's Secret Sauce recipe. She's been trailing the lead developer, Vick Timmes, to figure out how she can remotely access SaucyCorp's servers. One night, while conducting reconnaissance, she sees him log into his laptop (10.10.10.70) and VPN into SaucyCorp's headquarters.

Leveraging her connections with international hacking organizations, Ann obtains a 0-day exploit for Internet Explorer and launches a client-side spear phishing attack against Vick Timmes. Ann carefully crafts an email to Vick containing tips on how to improve secret sauce recipes and sends it. Seeing an opportunity that could get him that Vice President of Product Development title (and corner office) that he's been coveting, Vick clicks on the link. Ann is ready to strike…

Questions:

1. What was the full URI of Vick Timmes' original web request? (Please include the port in your URI.)
2. In response, the malicious web server sent back obfuscated JavaScript. Near the beginning of this code, the attacker created an array with 1300 elements labeled "COMMENT", then filled their data element with a string. What was the value of this string?
3. Vick's computer made a second HTTP request for an object. What was the filename of the object that was requested?
4. When was the TCP session on port 4444 opened? (for example : 49.5 seconds)
5. When was the TCP session on port 4444 closed?
6. In packet 17, the malicious server sent a file to the client : what type of file was it?
7. Vick's computer repeatedly tried to connect back to the malicious server on port 4445, even after the original connection on port 4444 was closed. With respect to these repeated failed connection attempts:
    a. How often does the TCP initial sequence number (ISN) change? (Every packet, Every third packet, Every 10-15 seconds, Every 30-35 seconds, Every 60 seconds)
    b. How often does the IP ID change?
    c. How often does the source port change?
8. Eventually, the malicious server responded and opened a new connection. When was the TCP connection on port 4445 first successfully completed? (for example : 49.5 seconds)
9. Subsequently, the malicious server sent an executable file to the client on port 4445. What was the MD5 sum of this executable file?
10. When was the TCP connection on port 4445 closed? (for example : 49.5 seconds)