Question 1

(a) First, we see that the initial step can be completed in K queries at most, and if this is the case, then the remaining problem becomes a search problem of finding K marked items in the list of N. Notice there will be some constraints on N for this case; if $K > N/2$, then we are guerenteed a collision in the set K, even in the worst case. Thus, for the most possible number of queries, we need $K \leq N/2$. In this case, we will get

$$O(K + \sqrt{N/K})$$

queries, where the first comes from the initial step, and the last order comes from the quantum search algorithm.

(b) Notice, if we choose $K = N^{1/3}$, we get

$$\implies O(N^{1/3} + \sqrt{N/N^{1/3}}) = O(N^{1/3} + \sqrt{N^{2/3}}) = O(2N^{1/3}) = O(N^{1/3})$$

as required.

Question 2

(a) First, we know the state in C is already $H^b|s\rangle$, so we only need to consider the states prepared in the A_1 and A_2 systems to understand what kind of density matrix we want. In particular, we know that Alice knows what s and b are, since that is how she prepares the state $H^b|s\rangle$. We see that

$$|s\rangle \otimes |b\rangle \otimes H^b|s\rangle \in A_1A_2C\,.$$

Therefore, the density matrix will be

$$|s\rangle\langle s| \otimes |b\rangle\langle b| \otimes H^b|s\rangle\langle s|H^b$$

since $(H^b)^\dagger = H^b$ in this case. Therefore, expanding each interms of their known components, we get

$$|s\rangle\langle s| \otimes |b\rangle\langle b| \otimes \frac{1}{2^b}\left(|+\rangle\langle 0| + |-\rangle\langle 1|\right)^b |s\rangle\langle s| \left(|+\rangle\langle 0| + |-\rangle\langle 1|\right)^b\,.$$

Further, we can eliminate the dependence on b by being clever with our construction, that is we can write

$$|b\rangle \otimes H^b|s\rangle = \frac{1}{\sqrt{2}}|0\rangle \otimes |s\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes H|s\rangle$$

which builds the dependence upon b into the state. So, the final density is

$$|s\rangle\langle s| \otimes \frac{1}{2}\left(|0\rangle\langle 0| \otimes |s\rangle\langle s| + |1\rangle\langle 1| \otimes H|s\rangle\langle s|H\right)\,,$$

where $H = \frac{1}{\sqrt{2}}(|+\rangle\langle 0| + |-\rangle\langle 1|)$.

(b) Eve has only caught the state in the system C, so we must have either

$$\rho_0 = \frac{1}{2}\left(|0\rangle\langle 0| + H|0\rangle\langle 0|H\right) \quad \& \quad \rho_1 = \frac{1}{2}\left(|1\rangle\langle 1| + H|1\rangle\langle 1|H\right)$$

(c) We use classical probability theory to see that we simply need to compute

$$P(s=e) = \frac{1}{2}\mathrm{Tr}\left(P_0\rho_0\right) + \frac{1}{2}\mathrm{Tr}(P_1\rho_1)$$

where

$$P_0\rho_0 = \frac{1}{2}\left(I + \frac{Z+X}{\sqrt{2}}\right)\frac{1}{2}\left(|0\rangle\langle 0| + H|0\rangle\langle 0|H\right)$$
$$= \frac{1}{4}\left(|0\rangle\langle 0| + H|0\rangle\langle 0|H + \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |1\rangle\langle 0|) + \frac{1}{\sqrt{2}}(ZH|0\rangle\langle 0|H + XH|0\rangle\langle 0|H)\right)$$

and so the trace of this thing would be

$$\frac{1}{4}\left(1 + \frac{1}{2} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}(\frac{1}{2}) + \frac{1}{2} + \frac{1}{2} + \frac{1}{\sqrt{2}}\left(-\frac{1}{2}\right) + \frac{1}{2}\right) = \frac{1}{4}\left(3 + \frac{1}{\sqrt{2}}\right)\,.$$

On the other hand, we have

$$P_1\rho_1 = \frac{1}{2}\left(I - \frac{Z+X}{\sqrt{2}}\right)\frac{1}{2}\left(|1\rangle\langle 1| + H|1\rangle\langle 1|H\right)$$

$$= \frac{1}{4}\left(I - \frac{Z+X}{\sqrt{2}}\right)\left(|1\rangle\langle 1| + H|1\rangle\langle 1|H\right)$$

$$= \frac{1}{4}\left(|1\rangle\langle 1| + H|1\rangle\langle 1|H - \frac{|1\rangle\langle 1| + |0\rangle\langle 1|}{\sqrt{2}} - \frac{1}{\sqrt{2}}\left(ZH|1\rangle\langle 1|H + XH|1\rangle\langle 1|H\right)\right)$$

$$= \frac{1}{4}\left(\frac{1}{2} - \frac{1}{\sqrt{2}}\left(\frac{1}{2} - \frac{1}{2}\right) + 1 + \frac{1}{2} - \frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}\left(-\frac{1}{2} - \frac{1}{2}\right)\right) = \frac{2}{4}$$

and thus the total will be

$$P(s=e) = \frac{1}{2}\left(\frac{1}{4}\left(3 + \frac{1}{\sqrt{2}}\right)\right) + \frac{1}{2}\left(\frac{1}{2}\right) = \frac{1}{8}\left(5 + \frac{1}{\sqrt{2}}\right)$$

as required.

(d) In this scenario, we are assuming $s = 0, b = 0$ and $e = 0$, so we can first find the post-measurement state to be

$$|\psi\rangle = \frac{P_0\rho_0 P_0}{\mathrm{Tr}(P_0\rho_0)} = \frac{1}{\frac{1}{4}\left(3 + \frac{1}{\sqrt{2}}\right)}\left(\frac{1}{2}\left(I + \frac{Z+X}{\sqrt{2}}\right)\frac{1}{2}\left(|0\rangle\langle 0| + H|0\rangle\langle 0|H\right)\left(\frac{1}{2}\left(I + \frac{Z+X}{\sqrt{2}}\right)\right)\right)$$

$$= \frac{4}{3 + \frac{1}{\sqrt{2}}}\frac{1}{8}\left(|0\rangle\langle 0| + H|0\rangle\langle 0|H + \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |1\rangle\langle 0|) + \frac{1}{\sqrt{2}}(ZH|0\rangle\langle 0|H + XH|0\rangle\langle 0|H)\right)\left(I + \frac{Z+X}{\sqrt{2}}\right)$$

Question 3

(a) This is just a matter of applying our definition of a matrix exponential. We recall that

$$e^{i\theta Z} = I\cos(\theta) + iZ\sin(\theta)$$

But, we notice that

$$D_1(\rho) = \frac{1}{2}e^{i\theta Z}\left(\rho e^{-i2\theta Z} + e^{-i2\theta Z}\rho\right)e^{i\theta Z}$$

and so we first compute the inner bracket to get

$$\rho e^{-i2\theta Z} + e^{-i2\theta Z}\rho = \rho\cos(2\theta) - i\rho Z\sin(2\theta) + \rho\cos(2\theta) - iZ\rho\sin(2\theta)$$

Notice that

$$\rho Z = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} a & -b \\ c & -d \end{pmatrix}$$
$$Z\rho = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ -c & -d \end{pmatrix}$$

So, we have

$$2\begin{pmatrix} a & b \\ c & d \end{pmatrix}\cos(2\theta) - 2i\sin(2\theta)\begin{pmatrix} a & 0 \\ 0 & -d \end{pmatrix} = 2\begin{pmatrix} a(\cos(2\theta) - i\sin(2\theta)) & b\cos(2\theta) \\ c\cos(2\theta) & d(\cos(2\theta) + i\sin(2\theta)) \end{pmatrix}.$$

So, we see that

$$\begin{aligned} D_1(\rho) &= 2\frac{1}{2}\begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix}\begin{pmatrix} a(\cos(2\theta) - i\sin(2\theta)) & b\cos(2\theta) \\ c\cos(2\theta) & d(\cos(2\theta) + i\sin(2\theta)) \end{pmatrix}\begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix} \\ &= 2\frac{1}{2}\begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix}\begin{pmatrix} ae^{-i\theta} & b\cos(2\theta)e^{-i\theta} \\ c\cos(2\theta)e^{i\theta} & de^{i\theta} \end{pmatrix} = \begin{pmatrix} a & b\cos(2\theta) \\ c\cos(2\theta) & d \end{pmatrix} \end{aligned}$$

as expected.

(b) First, we see that

$$Z\rho Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} a & -b \\ c & -d \end{pmatrix} = \begin{pmatrix} a & -b \\ -c & d \end{pmatrix}$$

and so we see that

$$D_2(\rho) = (1-p)\begin{pmatrix} a & b \\ c & d \end{pmatrix} + p\begin{pmatrix} a & -b \\ -c & d \end{pmatrix} = \begin{pmatrix} (1-p)a + pa & (1-p)b - pb \\ (1-p)c - pc & (1-p)d + pd \end{pmatrix} = \begin{pmatrix} a & (1-2p)b \\ (1-2p)c & d \end{pmatrix}$$

as expected.

(c) The easiest way to start this is to approach it using Dirac notation. In particular, we see we can represent our circuit as

$$(I \otimes |0\rangle\langle 0| + Z \otimes |1\rangle\langle 1|)(R \otimes I)(|0\rangle \otimes \rho = (R|0\rangle \otimes |0\rangle\langle 0| + ZR|0\rangle \otimes |1\rangle\langle 1|)(I \otimes \rho)$$

where we know

$$R|0\rangle = \sqrt{1-p}\,|0\rangle + \sqrt{p}\,|1\rangle \quad \& \quad ZR|0\rangle = \sqrt{1-p}\,|0\rangle - \sqrt{p}\,|1\rangle$$

and so

$$U = \begin{pmatrix} \sqrt{1-p} & 0 \\ \sqrt{p} & 0 \\ 0 & \sqrt{1-p} \\ 0 & -\sqrt{p} \end{pmatrix}$$

as required.

(d) We continue from where we left off, in that we know U, and we know how V must act on U, since it acts only in the E space, we must have that if

$$V = \begin{pmatrix} v_1 & v_2 \\ v_3 & v_4 \end{pmatrix}$$

then

$$(V \otimes I)U = \begin{pmatrix} \sqrt{1-p}v_1 + \sqrt{p}v_2 & 0 \\ \sqrt{1-p}v_3 + \sqrt{p}v_4 & 0 \\ 0 & \sqrt{1-p}v_1 - \sqrt{p}v_2 \\ 0 & \sqrt{1-p}v_3 - \sqrt{p}v_4 \end{pmatrix}.$$

So, if ρ is the arbitrary matrix from before, we are looking to find

$$\begin{pmatrix} \sqrt{1-p}v_1 + \sqrt{p}v_2 & 0 \\ \sqrt{1-p}v_3 + \sqrt{p}v_4 & 0 \\ 0 & \sqrt{1-p}v_1 - \sqrt{p}v_2 \\ 0 & \sqrt{1-p}v_3 - \sqrt{p}v_4 \end{pmatrix} \rho \left(\begin{pmatrix} \sqrt{1-p}v_1 + \sqrt{p}v_2 & 0 \\ \sqrt{1-p}v_3 + \sqrt{p}v_4 & 0 \\ 0 & \sqrt{1-p}v_1 - \sqrt{p}v_2 \\ 0 & \sqrt{1-p}v_3 - \sqrt{p}v_4 \end{pmatrix} \right)^T$$

$$= \begin{pmatrix} \sqrt{1-p}v_1 + \sqrt{p}v_2 & 0 \\ \sqrt{1-p}v_3 + \sqrt{p}v_4 & 0 \\ 0 & \sqrt{1-p}v_1 - \sqrt{p}v_2 \\ 0 & \sqrt{1-p}v_3 - \sqrt{p}v_4 \end{pmatrix}$$