60612100– Kiberxavfsizlik injiniringi ta’lim yo‘nalishi 4-bosqich talabalari uchun
Raqamli kriminalistika asoslari fanidan yakuniy nazorat savollari

1. Raqamli kriminalistika haqida umumiy ma’lumot bering.
2. Raqamli kriminalistika nima va uning klassik tergov usullaridan farqi nimada?
3. Raqamli kriminalistika fanining boshqa fanlar bilan bog‘liqligi haqida ma’lumot bering.
4. Raqamli kriminalistika va klassik tergov o‘rtasidagi asosiy farqlarni tushuntiring.
5. ISO 27037 standarti raqamli kriminalistikada qanday ahamiyatga ega?
6. Penetratsiya testerlar qanday vazifalarni bajaradi va ularga qanday bilimlar zarur?
7. Raqamli kriminalistika tarixi haqida ma’lumot bering.
8. Raqamli kriminalistika rivojiga ta'sir qilgan asosiy texnologik yutuqlarni sanab bering.
9. Raqamli tahlillar tasniflanishini tushuntirib bering.
10. Raqamli tergovchi qanday bilim va ko‘nikmalarga ega bo‘lishi kerak?
11. Raqamli kriminalistikada dalilning yaxlitligini saqlash nega muhim va bu qanday amalga oshiriladi?
12. Raqamli kriminalistikada foydalaniladigan asosiy dasturiy vositalarni tahlil qiling.
13. ASR Data va EnCase dasturlarining raqamli kriminalistikadagi o‘rni haqida ma’lumot bering.
14. Texnologik o‘zgarishlarning raqamli kriminalistika jarayoniga ta’sirini yoritib bering.
15. Forensic Toolkit (FTK) dasturining asosiy funksiyalari nimalardan iborat? Ularni izohlab bering.
16. Maxfiylik va shaxsiylik doirasidagi tushunchalar raqamli kriminalistikada qanday ahamiyatga ega?
17. Raqamli sud ekspertizasi resurslarini rivojlantirish jarayonini tushuntirib bering.
18. Raqamli kriminalistika va ma’lumotlarni tiklash tushunchalarini izohlang.
19. Tergovlar uchligi (uch guruh) konsepsiyasini batafsil tushuntiring. Har bir guruhning roli va ular o‘rtasidagi o‘zaro bog‘liqlikni izohlang.
20. Raqamli tahlillar uchun tayyorlanish jarayonini tushuntirib bering.
21. Samarali raqamli kriminalistika laboratoriyasini tashkil etishning asosiy bosqichlarini tushuntiring.
22. Raqamli kriminalistika laboratoriyasi uchun fizik talablarni tavsiflab bering.
23. Raqamli kriminalistika laboratoriyasi uchun asosiy ish stansiyasini tanlash mezonlarini tushuntiring.
24. Yuqori xavfli tergovlar uchun laboratoriyada ko‘riladigan maxsus xavfsizlik choralari haqida ma’lumot bering.
25. Raqamli kriminalistika laboratoriyasining byudjetini rejalashtirishda hisobga olinadigan omillarni tahlil qiling.
26. Sertifikatlash va malaka oshirish dasturlarining raqamli kriminalistika sohasi uchun ahamiyatini tushuntirib bering.
27. Raqamli kriminalistika laboratoriyasi menejeri va xodimlarining vazifalarini aniqlash jarayonini yoritib bering.
28. Laboratoriya uchun favqulodda holatlardan so‘ng tiklash rejasi qanday ishlab chiqiladi?
29. Raqamli kriminalistika laboratoriyasida dalil saqlash tizimining xavfsizligini ta’minlashda qanday usullar qo‘llaniladi?

30. Raqamli kriminalistika laboratoriyasida xavfsizlik auditi qanday tashkil etiladi va uning natijalari qanday qo‘llaniladi?
31. Laboratoriya jihozlarini tanlashda texnologik yangilanishlar va texnik muvofiqlik qanday hisobga olinadi?
32. Statik va dinamik nusxa olish usullarining farqlari va har birining afzallik hamda cheklovlarini tahlil qiling.
33. Raqamli dalillarni nusxalash jarayonida ochiq va yopiq manbali formatlardan foydalanish jarayonini tushuntirib bering.
34. Advanced Forensic Format (AFF) texnologiyasining raqamli tergovdagi ahamiyatini tuahuntirib bering.
35. Statik nusxa olish jarayonida dalilning yaxlitligini ta’minlash uchun ko‘riladigan choralar haqida ma’lumot bering.
36. Disk-to-image va disk-to-disk nusxa olish usullarining o‘zaro farqlarini tushuntirib bering.
37. Disk-to-image va disk-to-disk nusxa olish usullarini qaysi holatlarda foydalanish zaruratini tushuntirib bering.
38. Sparse acquisition usulining mohiyati va katta hajmli tizimlar bilan ishlashdagi afzalliklari haqida ma’lumot bering.
39. RAID tizimlarida ma’lumotlarni nusxalash va tahlil qilishning murakkab jihatlarini tushuntirib bering.
40. Windows va Linux muhitlarida raqamli dalillarni qo‘lga kiritish imkoniyatlarini solishtiring va har birining ustun jihatlarini tahlil qiling.
41. Mini-WinFE vositasi yordamida diskdan dalil olish jarayonini bosqichma-bosqich bayon qiling.
42. Raqamli kriminalistik vositalarning ishonchliligi va natijaning sudda e’tirof etilishi uchun qanday texnik shartlar bajarilishi zarur?
43. Raqamli tergovda ma’lumotlarni siqish usullari (lossless va lossy) va ularning qo‘llanilishi mumkin bo‘lgan kontekstlarni tushuntiring.
44. Raqamli tergovda ma’lumotlarni siqish usullari (lossless va lossy) va ularning qo‘llanilishi mumkin bo‘lgan kontekstlarini tushuntiring.
45. HPA (Host Protected Area) va uning raqamli tergovga ta’sirini tushuntirib bering.
46. BIOS, EFI va UEFI tizimlarining farqlari va ularning raqamli kriminalistik tekshiruvdagi ahamiyatini tushuntirib bering.
47. TEMPEST talablariga javob beradigan laboratoriyalar qanday hollarda zarur bo‘ladi?
48. High Tech Crime Network (HTCN) sertifikati haqida ma’lumot bering.
49. ISC2: Certified Cyber Forensics Professional (CCFP) dasturi haqida ma’lumot bering.
50. EnCase Certified Examiner (EnCE) sertifikati haqida ma’lumot bering.
51. Raqamli kriminalistika laboratoriyasi uchun xavfsizlik talablarini tavsiflab bering.
52. Raqamli kriminalistik ma’lumotlarni to‘plash tushunchasini tavsiflab bering.
53. Jinoyat joyida raqamli dalillarni to‘plash va qayta ishlash tartiblarini izohlang.
54. Raqamli dalillarning “chain of custody” (dalillarni uzluksiz nazorat qilish zanjiri) konsepsiyasini tushuntiring.
55. Raqamli kriminalistik ma’lumotlarni nusxalashda foydalaniladigan formatlarni tushuntirib bering.
56. Raqamli kriminalistik ma’lumotlarni qo‘lga kiritish usullari haqida ma’lumot bering.
57. Raqamli dalillarni aniqlash jarayonini tushuntirib bering.
58. Raqamli dalillar bilan ishlashda tergovchilarning umumiy vazifalari qaysilar?

59. Raqamli dalillarni xavfsiz saqlash va identifikatsiya qilish jarayonini tavsiflab bering.
60. Raqamli dalillar uchun xalqaro standartlarni o‘rnatish jarayoni dolzarbligini izohlang.
61. Microsoft fayl tuzilmalari haqida ma’lumot bering(sektorlar, klasterlar).
62. Microsoft fayl tuzilmalari haqida ma’lumot bering(fizik va mantiqiy manzillar).
63. Disk bo‘limlari (Partitions) haqida ma’lumot bering.
64. Disklarni tekshiruvchi maxsus dasturlar – WinHex yoki Hex Workshop haqida ma’lumot bering.
65. WinHex kabi Hex tahrirlovchi dasturlar yordamida o‘chirilgan fayllarni tiklash jarayoni qanday amalga oshiriladi?
66. CHS (Cylinder-Head-Sector) modelini tushuntirib bering.
67. File Allocation Table (FAT) – fayl tuzilmasi haqida ma’lumot bering.
68. File Allocation Table (FAT) – fayl tuzilmasi turlari(versiyalari) haqida ma’lumot bering.
69. Diskning foydalanilmagan maydoni(drive slack) mohiyatini tushuntirib bering.
70. File slack va RAM slack tushunchalarini tahlil qiling va ularning raqamli kriminalistik tekshiruvdagi ahamiyatini izohlang.
71. FAT16 fayl tizimi klasterlarida ma’lumotni joylashishini tushuntirib bering.
72. NTFS tizimidagi Master File Table (MFT) tuzilmasi va u orqali fayllar haqida qanday ma’lumotlarni olish mumkin?
73. NTFS tizimidagi Master File Table (MFT) tuzilmasi va u orqali fayllar haqida qanday ma’lumotlarni olish mumkin?
74. Raqamli kriminalistika vositalarini tanlashda qanday omillar hisobga olinadi, izohlab bering.
75. Apparat va dasturiy kriminalistika vositalarining o‘zaro farqlari va ularning afzalliklari hamda kamchiliklarini tahlil qiling.
76. Fayl sarlavhalarini tahlil qilish raqamli tergovlarda qanday rol o‘ynaydi?
77. Ekstraktsiya funksiyasining asosiy vazifalari nimalardan iborat?
78. Qayta tiklash (recovery) texnikasi qanday amalga oshiriladi va qanday hollarda diskni virtual yoki jismoniy tiklash afzal bo‘ladi?
79. Raqamli kriminalistika hisobotlari qanday shakllarda yaratiladi va bu hisobotlar tergovchi faoliyatini qanday qo‘llab-quvvatlaydi?
80. Shifrlangan fayllarni ochish qaysi vositalar orqali amalga oshiriladi?
81. Elektron pochta tahlilida "header" (sarlavha) ma'lumotlarining o‘rni qanday?
82. Elektron pochta orqali yuborilgan zararli faylni tahlil qilish jarayonini izohlang.
83. Ijtimoiy media tarmoqlarida foydalanuvchi faolligini kriminalistik tahlil qilishning asosiy bosqichlarini tavsiflab bering.
84. “Metadata” tushunchasi va uning email/ijtimoiy media tekshiruvlaridagi ahamiyati.
85. Elektron pochta orqali amalga oshirilgan fishing hujumlarini qanday aniqlash mumkin?
86. Ijtimoiy media profillarida saxta (fake) akkauntlarni aniqlash usullarini izohlang.
87. Elektron pochta serverlarining log fayllarini tahlil qilish jarayonini tushuntirib bering.
88. Internet of Things (IoT) tushunchasining raqamli kriminalistika amaliyotiga ta'sirini izohlab bering.
89. Mobil qurilmalarni tekshirishda mavjud bo'lgan muammolar va muhim qoidalar nimalardan iborat?
90. Mobil telefonlar va smartfonlar sud-ekspertizasi uchun qanday maxsus texnik va dasturiy vositalar talab qiladi?
91. Raqamli kriminalistika tergovlarida "scope creep" hodisasi qanday yuzaga keladi?

92. Raqamli dalillarni tekshirishda autopsy dasturi qanday foydalanuvchi imkoniyatlarni taqdim etadi?
93. Xodimlarning ish joyida elektron resurslarni noqonuniy foydalanish holatini aniqlashda qanday usullar qo‘llaniladi?
94. Raqamli dalillarni yig‘ishda qanday asosiy ehtiyot choralarini ko‘rish kerak.
95. Grafik fayllarni tahlil qilishda "hash" qiymatlarning ahamiyatini tushuntirib bering.
96. Grafik fayllarni siqish (compression) usullari haqida ma’lumot bering.
97. Raqamli kriminalistikada grafik fayllarni tiklashning asosiy usullari haqida ma’lumot bering.
98. Grafik faylda joylashgan Exif metadata soxtalashtirilganligini aniqlash yo’llarni tushuntirib bering.
99. JPEG formatida ishlatiladigan siqish mexanizmi qanday ishlashini tushuntirib bering.
100. Raqamli kriminalistika tergovlari uchun qanday saqlash vositalari tavsiya etiladi va ularga qo‘yiladigan xavfsizlik choralarini tushuntirib bering.