

O'ZBEKISTON RESPUBLIKASI OLIY TA'LIM, FAN VA
INNOVATSIYALAR VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT
TEKNOLOGIYALARI UNIVERSITETI



“TASDIQLAYMAN”

O'quv ishlari bo'yicha prorektor

Dj. Sultayev

2023-yil

Ro'yxatga olingan №

148

2023-yil

2.09

**MOBIL KRIMINALISTIKA
FANINING O'QUV DASTURI**

Bilim sohasi: 600000 – Axborot-kommunikatsiya
texnologiyalari

Ta'lim sohasi: 610000 – Axborot-kommunikatsiya
texnologiyalari

Mutaxassisligi: 70612101 – Raqamli kriminalistika

Fan/modul kodi	O'quv yili	Semestr	ESCTS kreditlar
1.06	2023-2024	2	6
Fan/modul turi	Ta'lim tili	Haftadagi dars soatlari	
majburiy	O'zbek/rus	4	
Fanning nomi	Auditoriya	Mustaqil ta'lim (soat)	Jami yuklama (soat)
1.		60	180
Mobil kriminalistika		120	
2.	<p>I. Fanning mazmuni <i>Fanni o'qitishdan maqsad</i> – talabalarda simsiz mobil aloqa tarmoqlari, mobil qurilmalar operatsion tizimlari, mobil qurilmalardan raqamli dalillarni qidirish usullari yo'nalishlari profiliga mos bilim, ko'nikma va malakani shakllantirishdan iborat.</p> <p><i>Fanning vazifasi</i> – talabalarda nazariy bilimlar, amaliy ko'nikmalar, mobil qurilmalar uchun mo'ljallangan iOS va Android operatsion tizimlarining ishlash prinsiplarini, iOS va Android operatsion tizimlarida ishlaydigan mobil qurilmalardan raqamli dalillarni qidirish usullarini, raqamli dalillarni qidirishdagi muammolarni tahlil qilishda ilmiy yondashuvni shakllantirishdan iborat.</p> <p>II. Asosiy nazariy qism (ma'ruza mashg'ulotlari) II.1. Fan tarkibiga quyidagi mavzular kiradi:</p> <p>1-mavzu. Mobil simsiz aloqa tarmoqlari Mobil tarmoqqa kirish. Uyali aloqa tarmoqlari: GSM, EDGE, UMTS, LTE va 5G texnologiyalari. IEEE 802.11 simsiz uzatish standartlari. Wi-Fi xavfsizligi.</p> <p>2-mavzu. Mobil qurilmalar va ularning operatsion tizimlari Antenna. DSP ortidagi matematika. SIM kartalar. Markaziy protsessor (CPU). Jammerlar, IMSI tutqichlari (IMSI Catchers).</p> <p>3-mavzu. iOS operatsion tizimi iOS operatsion tizimi asoslari. Jailbreaking. Fayl tizimi. iPhone smartfonlari sensorlari va protsessorlari. iPhone xavfsizligi.</p> <p>4-mavzular. Android operatsion tizimi. Android asoslari. Android telefon kalit kodlari. Android bilan ishlash. Android Debugging Bridge (ADB). Fayl tizimlari. Umumiy arxitekturasini.</p> <p>5-6-mavzular. iOS operatsion tizimli qurilmalar kriminalistikasi iOS operatsion tizimida kriminalistik jarayonlar. iOS operatsion tizimli qurilmalar uchun vositalar: Cellebrite, MobilEdit, iMyPhone, iCloud.</p>		

7-8-mavzular. Android operatsion tizimli qurilmalar kriminalistikasi.
Android operatsion tizimida kriminalistik jarayonlar. Android Debugging Bridge (ADB): /data, /cache, /misc, /mnt. Android operatsion tizimi uchun maxsus buyruqlar. iOS operatsion tizimli qurilmalar uchun vositalar: Autopsy, Bitpim, MobilEdit. Android ilovasini dekompiletsiya qilish.
8-10-mavzular. Birgalikda sinov harakat guruhi va o'chirish chipi JTAG. Chip-Off. Elektronika. Umumiy JTAG vositalari: RIFF, ORT BOX. Easy JTAG Box. JTAG standartlari: SWGDE, IEEE 1149, NIST, JTAG Guidance.
8-10-mavzular: Qo'ng'iroqlar tahlili va Smart TV kriminalistikasi Qo'ng'iroqlarni yozib olish qilish usullari. Smart televizorlar kriminalistikasi metodlari: Android Debugging Bridge (ADB) dan foydalanish, AnyDeskdan foydalanish.
11-12-mavzular. SQL ma'lumotlar bazasi kriminalistikasi. Relyatsion ma'lumotlar bazalari. Strukturaviy so'rovlar tili. SQLite asoslari. Google Chrome uchun SQLite Viewer. SQLite kriminalistikasi. SQLite Viewer.
13-14-15-mavzular. Kriminalistikaga qarshi himoya choralarlari Mobil qurilmalarni bloklash. Steganografiya: InvisibleSecrets, DeepSound. Simmetrik kriptografiya: DES, AES. Asimmetrik kriptografiya: RSA. Diffie-Hellman. Mobil qurilmaga xos kriptografiya. Xesh funksiyalar, Parolni buzish.
III. Amaliy mashg'ulotlar Amaliy mashg'ulotlar uchun quyidagi mavzular tavsiya etiladi:
1. Mobil qurilmalar, ularning tarkibiy qismlari va ishlash mexanizmi bilan tanishish.
2. Mobil operatsion tizimini virtual mashinaga o'rnatish va sozlash.
3. Firebase sinov laboratoriyasida iOS va Android operatsion tizimlarini sinovdan o'tkazish.
4-5. Android ilovalarini teskari muhandislik usuli yordamida tahlil qilishni amalga oshirish.
6. Kali Linuxda Andriллер dasturiy vositasi yordamida Android operatsion tizimida kriminalistik ekspertizasi amalga oshirish.
7. Autopsy mobil kriminalistika vositasi yordamida qattiq disk ustida amallar bajarish.
8-9. Mobil kriminalistika (Mobile Verification Toolkit) vositasi yordamida iOS va Android operatsion tizimli qurilmalarda ADB (Android Debugging Bridge) tekshiruvini amalga oshirish.

10-11. Metasploit Kali yordamida Android operatsion tizimli qurilmalarga ruxsatsiz kirish.

12-13. Magnet AXIOM vositasi yordamida iOS va Android operatsion tizimli qurilmalar uchun kriminalistik tahlilni amalga oshirish.

14-15. Oxygen Forensics vositasi yordamida jinoyatchilik harakatlarini kuzatish va tahlil qilish uchun dalillarni to'plash.

Amaliy mashg'ulotlar multimediya qurilmalari bilan jihozlangan auditoriyada bir akademik guruhga bir professor-o'qituvchi tomonidan o'tkazilishi zarur. Mashg'ulotlar faol va interaktiv usullar yordamida o'tilishi, mos ravishda munosib pedagogik va axborot texnologiyalar qo'llanilishi muqsadga muvofiq.

IV. Mustaqil ta'lim va mustaqil ishlar

Talabaga berilgan mustaqil ishning asosiy maqsadi – o'qituvchi rahbarligi va nazoratida muayyan o'quv ishlarini mustaqil ravishda bajarish uchun bilim va ko'nikmalarni shakllantirish va rivojlantirish.

Mustaqil ta'lim uchun tavsiya etiladigan mavzular:

1. iOS uchun maxsus vositalar tadqiqi: D-Back, Dr. Fone, Oxygen Forensics, iMazing, Axiom, Reincubate, Uldata.
2. iCloud xavfsizlik tizimi va uning imkoniyatlari
3. Android uchun maxsus vositalar tadqiqi: OSAF, Dual Use Tools, Cellebrite, Dr. Fone, Oxygen Forensics.

4. GrayKey dasturiy vositasi tadqiqi

5. Joint Test Action Group (JTAG) vositalari tahlili

6. JTAG standartlari tadqiqi

7. SQLITE FORENSIC EXPLORER dasturiy vositasi va uning imkoniyatlari

8. SQLite viewer (online) dasturiy vositasidan foydalanish

9. Systools SQLite viewer dasturiy vositasi va uning imkoniyatlari

10. Mobil bazaviy stansiyalar orqali jinoyatchini aniqlash usullari

11. Smart TV kriminalistikasi vositalari tahlili

12. Mobil qurilmalarni blokirovkasini ruxsatsiz ochish usullari

13. Mobil qurilmaga xos kriptografiya usullari

3. V. Fan o'qitilishining natijalari (shakllanadigan kompetentsiyalar)

Fanni o'zlashtirish natijasida talaba:

– simsiz mobil aloqa tarmoqlari, mobil qurilmalar operatsion tizimlari, mobil qurilmalardan raqamli dalillarni qidirish usullari amalda foydalanish haqida *tasavvurga ega bo'lishi*;

– mobil qurilmalar uchun mo'ljallangan iOS va Android operatsion tizimlarining ishlash prinsiplarini, iOS va Android operatsion tizimlarida ishlaydigan mobil qurilmalardan raqamli dalillarni qidirish usullarini, raqamli

dalillarni qidirishdagi muammolarni tahlil qilishni *bitishi va ulardan foydalana olishi*;

– mobil qurilmalardan raqamli dalillarni topishdagi muammolarni tahlil qilish, mobil kriminalistikaning zamonaviy usullaridan foydalanish, mobil qurilmalardan ma'lumotlarni tiklovchi dasturiy vositalardan foydalanish, ishlab chiqish va ularni takomillashtirish *ko'nikmalariga ega bo'lishi* kerak.

4. VI. Ta'lim texnologiyalari va metodlari:

- ma'ruzalar;
- interfaol keyslar-stadilar;
- seminarlar (mantiqiy fikrlash, tezkor savol javoblar);
- guruhlarda ishlash;
- taqdimotlarni qilish.

5. VII. Kredintlarni olish uchun talablar:

Fanga oid nazariy va uslubiy tushunchalarni to'la o'zlashtirish, tahlil natijalarini to'g'ri aks ettira olish, o'rganilayotgan jarayonlar haqida mustaqil mushohada yuritish va joriy va oraliq nazorat shakllarida berilgan vazifa va topshiriqlarni bajarish, yakuniy nazorat bo'yicha yozma ishni topshirish.

6. Asosiy adabiyotlar

1. Yusupov S.Y., Gulomov Sh.R., Nasrullayev N.B. Raqamli kriminalistika. "Aloqachi", - Toshkent 2020. **68**
2. S.K.Ganiev, A.A.Ganiev, Z.T.Xudoykulov. Kiberxavfsizlik asoslari: O'quv qo'llanma, – T. "Nihol print" OK, 2021. – 224 b. **69**

Qo'shimcha adabiyotlar

1. Chuck Easttom. AN IN-DEPTH GUIDE TO MOBILE DEVICE FORENSICS. 2022 Taylor & Francis Group, LLC. 249 –p.
2. Bill Nelson, Amelia Philips, Chris Steuart "Guide to computer forensics and investigation" – USA 2019, 770 bet.

Internet saytlari

1. <https://www.findresultsnow.co>
2. <http://www.lightmobile.com>
3. <https://www.lumatec.de>
4. <https://www.lookupsmart.com/>
5. <https://cellebrite.com/>
6. <https://www.geeksforgeeks.org>

7.	Fan dasturi Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Kengashining 2023-yil 30-avgustdagi 9(731)/1(732)-son bayonnomasi bilan tasdiqlangan.
8.	Fan/modul uchun ma'sullar: Allanov Orif Menglimuratovich – Muxammad al-Xorazmiy nomidagi TATU, “Kiberxavfsizlik va kriminalistika” kafedrasi mudiri, PhD.
9.	Taqrizchilar: Z.T. Xudoyqulov – Muxammad Al-Xorazmiy nomidagi TATU, “Kriptologiya” kafedrasi mudiri, PhD (turdosh OTM). I.M. Bouquziyev– Renessans ta'lim universiteti, “Matematika va axborot texnologiyalari” kafedrasi PhD, dotsent. (turdosh OTM).